March 18, 2015

Dear [Redacted]

Re: Your request for access to information under Part II of the Access to Information and Protection of Privacy Act [Our File #: OPE/1/2015]

On January 27, 2015 the Office of Public Engagement received your request for access to the following records/information:


On February 23, 2015 we advised you that the 30 day time period for responding to your request had been extended for an additional 30 days, in accordance with subsection 16(1)(d) of the Act, as consultations with other public bodies were required.

I am pleased to inform you that your request for access to these records has been granted in part. In particular, access is granted to the 43 privacy breach reports that were submitted to the ATIPP Office during the requested period with limited information being withheld.

Access to the remaining information contained within the records, has been refused in accordance with the following exceptions to disclosure, as specified in the Access to Information and Protection of Privacy Act (the Act):

22(1) The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to
   (a) interfere with or harm a law enforcement matter;
   (i) reveal the arrangements for the security of property or a system, including a
       building, a vehicle, a computer system or a communications system;

23(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to
   (a) harm the conduct by the government of the province of relations between that
       government and the following or their agencies:
       (iii) the government of a foreign state,

24(1) The head of a public body may refuse to disclose to an applicant information which could reasonably be expected to disclose
   (g) information, the disclosure of which could reasonably be expected to prejudice the
       financial or economic interest of the government of the province or a public body.
30(1) The head of a public body shall refuse to disclose personal information to an applicant where the disclosure would be an unreasonable invasion of a third party's personal privacy.

Please note that the responsibility for determining how to document and respond to privacy breaches lies with each public body and the current legislation does not require that public bodies submit privacy breach reports to the ATIPP Office. Therefore, there may be breaches that occurred during the 2011-12 fiscal year where the ATIPP Office did not receive reports.

As required by subsection 7(2) of the Act, we have severed information that is excepted from disclosure and have provided you with as much information as possible. In accordance with your request for a copy of the records, the appropriate copies have been enclosed.

Section 43 of the Act provides that you may ask the Information and Privacy Commissioner to review this partial refusal of access or you may appeal the refusal to the Supreme Court Trial Division. A request to the Information and Privacy Commissioner shall be made in writing within 60 days of the date of this letter or within a longer period that may be allowed by the Commissioner.

The address and contact information of the Information and Privacy Commissioner is as follows:

Office of the Information and Privacy Commissioner
2 Canada Drive
P. O. Box 13004, Stn. A
St. John's, NL. A1B 3V8

Telephone: (709) 729-6309
Facsimile: (709) 729-6500

In the event that you choose to appeal to the Trial Division, you must do so within 30 days of the date of this letter. Section 60 of the Act sets out the process to be followed when filing such an appeal.

Please be advised that responsive records will be published following a 72 hour period after the response is sent electronically to you or five business days in the case where records are mailed to you. It is the goal to have the responsive records posted to the Office of Public Engagement's website within one business day following the applicable period of time. Please note that requests for personal information will not be posted online.

If you have any further questions, please contact the ATIPP Coordinator, Sonja El-Gohary, at 709-729-7128, or sonjaelgohary@gov.nl.ca.

Sincerely,

JUDITH HEARN
Deputy Minister
# OPE/1/2015: INDEX OF PRIVACY BREACH REPORTS SUBMITTED TO THE ATIPP OFFICE DURING THE 2011-12 FISCAL YEAR (APRIL 1, 2011 – MARCH 31, 2012)

<table>
<thead>
<tr>
<th>#</th>
<th>Public Body*</th>
<th>Date submitted to ATIPP Office</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Government Services</td>
<td>April 7, 2011</td>
<td>1-5</td>
</tr>
<tr>
<td>2.</td>
<td>Government Services</td>
<td>April 15, 2011</td>
<td>6-10</td>
</tr>
<tr>
<td>5.</td>
<td>Government Services</td>
<td>May 2, 2011</td>
<td>21-25</td>
</tr>
<tr>
<td>9.</td>
<td>Human Resources, Labour and Employment</td>
<td>June 1, 2011</td>
<td>41-45</td>
</tr>
<tr>
<td>17.</td>
<td>Government Services</td>
<td>August 17, 2011</td>
<td>81-85</td>
</tr>
<tr>
<td>19.</td>
<td>Public Service Commission</td>
<td>August 26, 2011</td>
<td>91-93</td>
</tr>
<tr>
<td>23.</td>
<td>Government Services</td>
<td>September 20, 2011</td>
<td>109-113</td>
</tr>
<tr>
<td>24.</td>
<td>Government Services</td>
<td>September 23, 2011</td>
<td>114-118</td>
</tr>
<tr>
<td>25.</td>
<td>Government Services</td>
<td>September 27, 2011</td>
<td>119-123</td>
</tr>
<tr>
<td>27.</td>
<td>Government Services</td>
<td>October 5, 2011</td>
<td>129-133</td>
</tr>
<tr>
<td>29.</td>
<td>Government Services</td>
<td>October 6, 2011</td>
<td>139-143</td>
</tr>
<tr>
<td>30.</td>
<td>Government Services</td>
<td>October 17, 2011</td>
<td>144-148</td>
</tr>
<tr>
<td>32.</td>
<td>Education</td>
<td>October 24, 2011</td>
<td>154-158</td>
</tr>
<tr>
<td>33.</td>
<td>Government Services</td>
<td>October 26, 2011</td>
<td>159-163</td>
</tr>
<tr>
<td>34.</td>
<td>Government Services</td>
<td>November 21, 2011</td>
<td>164-168</td>
</tr>
<tr>
<td>35.</td>
<td>College of the North Atlantic</td>
<td>November 24, 2011</td>
<td>169-173</td>
</tr>
<tr>
<td>36.</td>
<td>Service NL</td>
<td>December 1, 2011</td>
<td>174-178</td>
</tr>
<tr>
<td>37.</td>
<td>Government Services</td>
<td>December 1, 2011</td>
<td>179-183</td>
</tr>
<tr>
<td>38.</td>
<td>College of the North Atlantic</td>
<td>December 8, 2011</td>
<td>184-188</td>
</tr>
<tr>
<td>#</td>
<td>Public Body*</td>
<td>Date submitted to ATIPP Office</td>
<td>Pages</td>
</tr>
<tr>
<td>----</td>
<td>---------------------------------------</td>
<td>-------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>39.</td>
<td>Service NL</td>
<td>December 19, 2011</td>
<td>189-193</td>
</tr>
<tr>
<td>40.</td>
<td>Service NL</td>
<td>December 22, 2011</td>
<td>194-198</td>
</tr>
<tr>
<td>41.</td>
<td>Service NL</td>
<td>December 29, 2011</td>
<td>199-203</td>
</tr>
<tr>
<td>42.</td>
<td>Advanced Education and Skills</td>
<td>January 4, 2011</td>
<td>204-208</td>
</tr>
<tr>
<td>43.</td>
<td>Service NL</td>
<td>February 1, 2012</td>
<td>209-213</td>
</tr>
</tbody>
</table>

* Human Resources, Labour and Employment is now known as Advanced Education and Skills; Government Services is now known as Service NL; Justice is now known as Justice and Public Safety; Education is now known as Education and Early Childhood Development; Nova Central and Eastern School Districts are now part of the NL English School District;
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckettg@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: April 7, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
**Risk Evaluation**

**Incident Description**

1. Date the breach occurred: shortly after February 12, 2011
2. Date the breach was discovered: March 30, 2011
3. Describe the breach (provide sufficient detail, including cause):
   
   The Transportation and Works Mail Room in the Confederation Building mailed a vehicle registration renewal notice to a customer. Included with this document, which was torn, was the registration renewal notice for a different individual.
4. Location of the breach:
   Confederation Building
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   - [x] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   
   The vehicle registration renewal notice for the third party was given to her by the individual who received it. The individual whose personal information was disclosed was contacted with an apology and the offer of a new driver licence number and vehicle plate number.

**Personal Information Involved**

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information**:
   
   Name, full address, driver's licence number, Vehicle Plate Number, Registration Expiry Date, Make/Model/Colour/Mass/Year of vehicle, Renewal Fee, Vehicle Serial Number. At this point in time, we are unable to determine whether there were any outstanding fines disclosed, however, given these are publically available through the court system, they do not qualify as ATIPP breach.

**Safeguards**

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   There is a sensor in the mailing machine used to check that only single copies of the page are inserted into each envelop. Transportation and Works has recently been having problems whereby the new government logo in the top left hand corner of some forms
causes confusion for the sensor. MRD will review the logo location on all forms which go through the Transportation and Works mailing system to ensure sensor confusion is eliminated.

As a precaution against double stuffing envelops, the TW mail room also has a physical count of the number of documents to be placed into envelops and is to compare this number with the number of envelops run through the stuffing machine. In this case, this precaution did not work.

10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:

All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [x] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes  Date Analyst was notified:  April 6, 2011
   - [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes  Who was notified and when?
   - [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

**IMPORTANT!** Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

___________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckettt@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: April 15, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
**Risk Evaluation**

**Incident Description**

1. Date the breach occurred: April 11, 2011
2. Date the breach was discovered: April 13, 2011
3. Describe the breach (provide sufficient detail, including cause):
   
   The Motor Registration Division mailed a vehicle registration renewal and sticker to a customer. Included with these documents were two registration renewals and one sticker for a different individual.

4. Location of the breach:
   
   Mount Pearl

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One

6. Type(s) of individuals affected (check all that apply):
   
   - [x] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   
   The vehicle registrations and one sticker for two vehicles mailed in error were returned to MRD and then mailed on to the correct owner. The client affected has been advised by telephone and accepted our offer to obtain a new driver licence number and a new licence plate for the car. A letter of apology will be sent today.

**Personal Information Involved**

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information**:
   
   Name, full address, driver’s licence number, Vehicle Plate Numbers, Sticker Number, Document Generation Date, Registration Expiry Date, Make/Model/Style/Colour/Mass/Year/Fuel of two vehicles, Fees paid, Vehicle Serial Numbers

**Safeguards**

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   
   , N/A

10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to take due care in mailings.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [ ] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] Physical harm or harassment (e.g. stalking)
   - [ ] Emotional harm, humiliation or damage to reputation (e.g. disclosure of mental health records)
   - [ ] Financial cost
   - [ ] Loss of business or employment opportunities
   - [ ] Breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] Future breaches (technical failures)
   - [ ] Violation of professional standards or certificate standards
   - [ ] Risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [ ] Yes Date Analyst was notified: April 14, 2011
   - [ ] No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes Who was notified and when?
   - [ ] No Will law enforcement be notified at a later time?
     - [ ] Yes
     - [ ] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes Who was notified and when?
   - [ ] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes Who was notified and when?
   - [ ] No Will other authorities be notified at a later time?
     - [ ] Yes
     - [ ] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: HRLE

Division / Program: Avalon Region

Contact:

Name: Lori Rose
Title: Regional Manager
Phone: 729-7883
Fax: 729-3018
E-Mail: lorirose@gov.nl.ca
Mailing address: Avalon Regional Office 261 Kenmount Road
Box 8700, St. John's, NL, A1B 4J6

Date of Submission to the ATIPP Office: May 2, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: April 29, 2011
2. Date the breach was discovered: April 29, 2011
3. Describe the breach (provide sufficient detail, including cause):
   When responding to a client's email, a worker sent the response to an incorrect email address.
4. Location of the breach:
   Metro Place
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 1
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc.):
   The worker realized immediately that an error had been made, and she sent a recall notice to recall the email. Unfortunately the other party had already opened and viewed the email. Contact was then made with the other party to explain the error and we requested that the email be deleted. The email recipient agreed to delete the message she had received. Contact was also made with the client whose information had been compromised. The error was explained in detail and the client was very understanding of the incident.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Personal information involved included: name, address, HRLE file number and SIN

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   n/a
10. Describe the administrative safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:
We have a policy that we do not provide any information on a file in response to an email until we can verify the identity of the sender. We require 3 identifying pieces of information - name, HRLE file # and last three digits of the SIN. Since this incident we have met with our email team to stress due diligence when responding to emails to ensure that the correct address is selected.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [ ] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - ☒ Identify theft (higher risk if breach involves SIN # or financial information)
   - ☐ physical harm or harassment (e.g. stalking)
   - ☐ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - ☐ financial cost
   - ☐ loss of business or employment opportunities
   - ☐ breach of contract (e.g. from data loss)
   - ☐ future breaches (technical failures)
   - ☐ violation of professional standards or certificate standards
   - ☐ risk to public health or safety
   - ☐ Other (please specify):  

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - ☒ Yes   Date Analyst was notified:  May 2, 2011
   - ☐ No   When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - ☐ Yes   Who was notified and when?
   - ☒ No   Will law enforcement be notified at a later time?
     - ☐ Yes
     - ☒ No

15. Have other authorities (E.g. professional bodies) been contacted?
   - ☐ Yes   Who was notified and when?
   - ☒ No   Will other authorities be notified at a later time?
     - ☐ Yes
     - ☒ No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: HRLE

Division / Program: Avalon Region

Contact:

Name: Lori Rose
Title: Regional Manager
Phone: 729-7883
Fax: 729-3018
E-Mail: lorirose@gov.nl.ca
Mailing address: Avalon Regional Office 261 Kenmount Road Box 8700, St. John's, NL, A1B 4J6

Date of Submission to the ATIPP Office: May 2, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: April 26, 2011
2. Date the breach was discovered: April 27, 2011
3. Describe the breach (provide sufficient detail, including cause):
   Client information was faxed to the Special Assistance Program warehouse with Eastern Health instead of Eastern Health's Office of the Special Assistance Program.
4. Location of the breach:
   Metro Place
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 5
6. Type(s) of individuals affected (check all that apply):
   □ Client / Customer / Patient
   □ Employee
   □ Student
   □ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   Information was immediately retrieved by an HRLE employee and routed properly. Upon investigation of this incident, we determined that a recent memo from Eastern Health caused some confusion for staff around a change in fax numbers. This has since been clarified for staff.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Personal information involved included: name, address, date of birth, MCP numbers, and limited medical history.

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   n/a
10. Describe the administrative safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:
    An email has been sent to staff clarifying the correct fax numbers for Eastern Health services.
11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [ ] Encryption
- [ ] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - □ Identify theft (higher risk if breach involves SIN # or financial information)
   - □ physical harm or harassment (e.g. stalking)
   - □ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - □ financial cost
   - □ loss of business or employment opportunities
   - □ breach of contract (e.g. from data loss)
   - □ future breaches (technical failures)
   - □ violation of professional standards or certificate standards
   - □ risk to public health or safety
   - ☑ Other (please specify): Risk of harm is minimal in this incident as the information was still within Eastern Health.

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - ☑ Yes Date Analyst was notified: May 2, 2011
   - □ No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - □ Yes Who was notified and when?
   - ☑ No Will law enforcement be notified at a later time?
     - □ Yes
     - ☑ No

15. Have other authorities (E.g. professional bodies) been contacted?
   - □ Yes Who was notified and when?
   - □ No Will other authorities be notified at a later time?
     - □ Yes
     - ☑ No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckettt@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: May 2, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: April 21, 2011
2. Date the breach was discovered: April 26, 2011
3. Describe the breach (provide sufficient detail, including cause):
   An Automobile Dealer keyed the wrong information with respect to a customer and submitted this through the Dealer Web registration system. The MRD system generated a new driver licence based upon a changed address and sent the new licence to a third party.
4. Location of the breach:
   Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   ☑ Client / Customer / Patient
   ☐ Employee
   ☐ Student
   ☐ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   The driver licence was apparently cut up by the third party. The third party is suspicious of someone attempting to steal their identity and will be offered a new driver licence number. The client affected has been advised by telephone and accepted our offer to obtain a new driver licence number. A letter of apology will be sent to the client affected.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, driver's licence number, photo, driver class, date of birth, gender, eye colour, height, date of first licence, signature

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   , N/A
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. A letter will be sent by the Registrar of Motor Vehicles to all automobile dealers using the Dealers Web requesting their cooperation in ensuring accurate information on web transactions.

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [x] Encryption
- [x] Password
- [ ] Other (please specify):

Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [x] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes Date Analyst was notified: May 2, 2011
   - [ ] No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [x] Yes Who was notified and when? Constable Doug Pike was advised by the party who received the driver licence on April 26, 2011. Apparently, at this time the party 'heard' he was to cut up the licence. On May 2, Constable Pike confirmed there was no further investigation to be carried out by the RNC.
   - [ ] No Will law enforcement be notified at a later time?
      - [ ] Yes
      - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes Who was notified and when?
   - [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes Who was notified and when?
   - [x] No Will other authorities be notified at a later time?
      - [ ] Yes
      - [x] No
Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of
individuals affected by the privacy breach. Please review the Notification Assessment Tool that
is available from the ATIPP Office website:
http://www.justice.gov.nl.ca/just/civil/atipp/

For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach
Reporting form and apply a “Date Received” stamp, in the space provided below. The form must
then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

**Contact Information**

**Department / Public Body:** HRLE

**Division / Program:** Finance

**Contact:**

Name: Janelle Kenway  
Title: PPDS  
Phone: 729-7920  
Fax:  
E-Mail: janellekenway@gov.nl.ca  
Mailing address: 3rd Floor West Block Confederation Building

**Date of Submission to the ATIPP Office:** May 13, 2011

*(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)*
Risk Evaluation

Incident Description

1. Date the breach occurred: April 2011
2. Date the breach was discovered: May 10, 2011
3. Describe the breach (provide sufficient detail, including cause):
   Finance division sends out notices to local service districts advising them of individuals on Income Support because HRLE pays their municipal taxes. In this instance - the local service district is now dissolved and the client information needs to be mailed to a different address.
4. Location of the breach:
5. Estimated number of individuals directly affected by the privacy breach (i.e., whose personal information has been compromised): 2
6. Type(s) of individuals affected (check all that apply):
   □ Client / Customer / Patient
   □ Employee
   □ Student
   □ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g., retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   The information was sent back to HRLE

Personal Information Involved

8. Describe the personal information involved (e.g., name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   The only information contained on the report was the client's name and address and the fact they were receiving income support.

Safeguards

9. Describe the physical safeguards (e.g., locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   N/A
10. Describe the administrative safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:
    We should consult / interface with Municipal Affairs to ensure we know of all Local Service District Changes
11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:
Encryption
Password
Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - Identify theft (higher risk if breach involves SIN # or financial information)
   - physical harm or harassment (e.g. stalking)
   - emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - financial cost
   - loss of business or employment opportunities
   - breach of contract (e.g. from data loss)
   - future breaches (technical failures)
   - violation of professional standards or certificate standards
   - risk to public health or safety
   - Other (please specify): It makes HRLE look irresponsible for sending the information to the wrong location.

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - Yes Date Analyst was notified: May 10, 2011
   - No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - Yes Who was notified and when?
   - No Will law enforcement be notified at a later time?
     - Yes
     - No

15. Have other authorities (E.g. professional bodies) been contacted?
   - Yes Who was notified and when?
   - No Will other authorities be notified at a later time?
     - Yes
     - No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body:  HRLE

Division / Program:  Income Support

Contact:

Name:  Janelle Kenway
Title:  PPDS
Phone:  729-7920
Fax:
E-Mail:  janellekenway@gov.nl.ca
Mailing address:  3rd Floor West Block Confederation Building

Date of Submission to the ATIPP Office:  May 13, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: May 11, 2011
2. Date the breach was discovered: May 11, 2011
3. Describe the breach (provide sufficient detail, including cause):

   A new applicant to Income Support, [redacted], who lives in [redacted] with postal code [redacted] called into HRLE and wondered where his cheque was. The CSO who answered the phone got him confused with another client - [redacted], who is also on income support and lives in [redacted] with Postal code [redacted]. Both individuals have the same box number and both live with their grandparents.

   [redacted] received a mail back form in error and filled it out - and didn’t realize that he didn’t need to fill it out or that it wasn’t his. There is nothing of concern on the mail back form.

   We did not notify the clients as there was no identifying information on the forms. Staff are now asked to check for 2 pieces of identifying information.

4. Location of the breach:
   Western NL

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 2

6. Type(s) of individuals affected (check all that apply):
   ☑ Client / Customer / Patient
   ☐ Employee
   ☐ Student
   ☐ Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):

   Staff are asked to ask for 2 identifying pieces of information when speaking to clients for verification.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   name and address

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
10. Describe the **administrative** safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:

   CSOs usually ask for 1 piece of information to confirm identity

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

   ☐ Encryption
   ☐ Password
   ☐ Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - Identify theft (higher risk if breach involves SIN # or financial information)
   - physical harm or harassment (e.g. stalking)
   - emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - financial cost
   - loss of business or employment opportunities
   - breach of contract (e.g. from data loss)
   - future breaches (technical failures)
   - violation of professional standards or certificate standards
   - risk to public health or safety
   - Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - Yes Date Analyst was notified: May 11, 2011
   - No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - Yes Who was notified and when?
   - No Will law enforcement be notified at a later time?
     - Yes
     - No

15. Have other authorities (E.g. professional bodies) been contacted?
   - Yes Who was notified and when?
   - No Will other authorities be notified at a later time?
     - Yes
     - No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:
http://www.justice.gov.nl.ca/just/civil/atipp/
For **Internal Use by the ATIPP Office Only**

Date Reporting form received by the ATIPP Office:

**IMPORTANT!** Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

---

**Received by:**

________________________

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: HRLE

Division / Program: Income Support

Contact:

Name: Janelle Kenway
Title: PPDs
Phone: 729-7920
Fax:
E-Mail: janellekenway@gov.nl.ca
Mailing address: 3rd Floor West Block, Confederation Building

Date of Submission to the ATIPP Office: May 13, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: May 10, 2011
2. Date the breach was discovered: May 10, 2011
3. Describe the breach (provide sufficient detail, including cause):
   A client consent form was printed from CAP (CITRIX) database and was sent to the wrong office (povery reduction). CITRIX has been having many issues and staff have been advised twice on the protocols to follow when they notice their print job does not appear at their default printer.
4. Location of the breach:
   Avalon Region
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 1
6. Type(s) of individuals affected (check all that apply):
   - [ ] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   Another memo is being sent to staff on the steps to follow for a CITRIX breach.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name of client and address

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   Information that arrives at the wrong destination printer will be reported to PPE and then shredded
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
    Employees are asked to check to ensure they receive their print jobs
11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:
☐ Encryption
☐ Password
☒ Other (please specify): OCIO is trying to fix the CITRIX system
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - Identify theft (higher risk if breach involves SIN # or financial information)
   - physical harm or harassment (e.g. stalking)
   - emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - financial cost
   - loss of business or employment opportunities
   - breach of contract (e.g. from data loss)
   - future breaches (technical failures)
   - violation of professional standards or certificate standards
   - risk to public health or safety
   - Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - Yes    Date Analyst was notified: May 10, 2011
   - No     When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - Yes    Who was notified and when?
   - No     Will law enforcement be notified at a later time?
   - Yes
   - No

15. Have other authorities (E.g. professional bodies) been contacted?
   - Yes    Who was notified and when?
   - No     Will other authorities be notified at a later time?
   - Yes
   - No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

______________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Human Resources, Labour & Employment

Division / Program: Income Support

Contact:

Name: Stephanie Baker or Dale Murphy
Title: Client Services Manager (IS); Client Services Manager - Corporate Services
Phone: 709-637-2475
Fax: 709-637-2931
E-Mail: stephaniebaker@gov.nl.ca; dalemurphy@gov.nl.ca
Mailing address: P O Box 2006, 1-3 Union Street, 2nd floor, Corner Brook, NL A2H 6J9

Date of Submission to the ATIPP Office: June 1st 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: June 1, 2011
2. Date the breach was discovered: June 1, 2011
3. Describe the breach (provide sufficient detail, including cause):
   Income Support Job Start cheque issued to a CEYS client awaiting LMAPD funding
4. Location of the breach:
   Corner Brook
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 1
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   Visually impaired client inadvertently provided with a job start cheque issued for another client. Cheque has been retrieved by the bank. Client who was given the incorrect cheque was explained what occurred. I (Stephanie Baker) attempted to make contact with client whose confidentiality has been breached but unsuccessful to date. File updated and case note entered directing inquiries to me.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Cheque with client name, home address and case number.

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   Cheques are kept in a locked cabinet for front office use.
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
   Clients who pick up cheques must provide 2 pieces of identification and sign form to accept cheque. In this instance, human error lead to incorrect cheque being released.
11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:
 Encryption
 Password
 Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

- Identity theft (higher risk if breach involves SIN # or financial information)
- Physical harm or harassment (e.g. stalking)
- Emotional harm, humiliation or damage to reputation (e.g. disclosure of mental health records)
- Financial cost
- Loss of business or employment opportunities
- Breach of contract and/or other legal obligations (e.g. from data loss)
- Future breaches (technical failures)
- Violation of professional standards or certificate standards
- Risk to public health or safety
- Other (please specify): risk is minimal although cheque does confirm client was in receipt of a job start cheque from the income support program with hrle and provides client name & address

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

- Yes Date Analyst was notified:
- No When will the Analyst be notified? via this email

14. Have law enforcement officials been notified?

- Yes Who was notified and when?
- No Will law enforcement be notified at a later time?
  - Yes
  - No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?

- Yes Who was notified and when?
- No

16. Have other authorities (e.g. professional bodies) been contacted?

- Yes Who was notified and when?
- No Will other authorities be notified at a later time?
  - Yes
  - No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

**IMPORTANT!** Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

_________________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Human Resources, Labour and Employment

Division / Program: Income Support / Accounts Receivable

Contact:

Name: Ellen Foley
Title: Client Service Manager
Phone: 709-256-1238
Fax: 256-1251
E-Mail: ellenfoley@gov.nl.ca
Mailing address: 230 Airport Blvd Gander

Date of Submission to the ATIPP Office: June 2, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: May 30, 2011
2. Date the breach was discovered: May 31, 2011
3. Describe the breach (provide sufficient detail, including cause):
   A file was split for an overpayment when a couple separated. The new file that was set up for the male individual was for the wrong person. As a result, he received an overpayment notice that was not his. This occurred when the file was set up in CAPS.
4. Location of the breach:
   Central Region - Marystown and Clarenville Individuals affected
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 2
6. Type(s) of individuals affected (check all that apply):
   - [x] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   Retrieved the letters and information sent to the wrong client.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information:**

   Information would have included address, SIN, marital status

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   Files are kept in locked cabinets
10. Describe the administrative safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:

    Collection officers should verify information using SIN and client ID - not names as there are many individuals in NL with the same name.
11. Describe the technical safeguards (access controls, audit controls, etc...) currently in place to protect the personal information in your custody and control:

    - [ ] Encryption
☐ Password
☐ Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [x] Identify theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [x] emotional harm, humiliation or damage to reputation (e.g. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes Date Analyst was notified: May 31, 2011
   - [ ] No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [x] Yes Who was notified and when?
   - [x] No Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have other authorities (E.g. professional bodies) been contacted?
   - [x] Yes Who was notified and when?
   - [x] No Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

**IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.**


Received by:

________________________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body:  Nova Central School District [Heather Hillier, SAO (Corporate Services), hhillier@ncsd.ca/709-256-2547, ext. 298]

Division / Program:  St. Stephen’s All Grade

Contact:

Name:  Kyle Smith
Title:  Principal
Phone:  848-3516
Fax:  848-3106
E-Mail:  KyleSmith@ncsd.ca
Mailing address:  P.O. Box 59, Rencontre East, NL  A0H 2C0

Date of Submission to the ATIPP Office:  June 10, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
**Risk Evaluation**

**Incident Description**

1. Date the breach occurred:  June 7, 2011
2. Date the breach was discovered:   June 8, 2011
3. Describe the breach (provide sufficient detail, including cause):
   
   Information from inactive files, old documents and school registers was inappropriately sent to the local dump without being shredded. The matter was brought to the attention of the school district by a student who discovered the materials at the dump.

4. Location of the breach:
   
   Rencontre East

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised):  50

6. Type(s) of individuals affected (check all that apply):
   
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   
   - The principal went immediately to the dump to retrieve the discarded materials.

**Personal Information Involved**

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history).  **Do not include or send us the identifiable personal information:**
   
   - Names
   - Dates of Birth
   - Contact information
   - MCP numbers
   - Evaluation data (e.g. marks for tests & assignments)
   - Student work
   - Attendance data
   - Correspondence and other items from student files.

**Safeguards**

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
- Locked cabinets & locked rooms

10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
   - Staff training & awareness
   - ATIPPA brochure distributed to schools/staff
   - Limited access to personal information in files
   - Student Records policy

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

   - Encryption
   - Password
   - Other (please specify): Remote access via main server
**Potential Harm**

12. Identify any harm that may result from the breach (check all that apply):

- [ ] Identify theft (higher risk if breach involves SIN # or financial information)
- [ ] physical harm or harassment (e.g. stalking)
- [x] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
- [ ] financial cost
- [ ] loss of business or employment opportunities
- [ ] breach of contract (e.g. from data loss)
- [ ] future breaches (technical failures)
- [ ] violation of professional standards or certificate standards
- [ ] risk to public health or safety
- [ ] Other (please specify):

**Notification**

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

- [x] Yes Date Analyst was notified: June 8, 2011
- [ ] No When will the Analyst be notified?

14. Have law enforcement officials been notified?

- [ ] Yes Who was notified and when?
- [x] No Will law enforcement be notified at a later time?

- [ ] Yes
- [x] No

15. Have other authorities (E.g. professional bodies) been contacted?

- [ ] Yes Who was notified and when?
- [x] No Will other authorities be notified at a later time?

- [ ] Yes
- [x] No

**Important!**

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the **Notification Assessment Tool** that is available from the ATIPP Office website:

For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

department / public body: government services

Division / Program: Government Service Centre

Contact:

Name: Robert Groves
Title: Manager of Operation
Phone: 466-4064
Fax: 466-5674
E-Mail: rgroves@gov.nl.ca
Mailing address: 8 Myer's Avenue

Date of Submission to the ATIPP Office: June 13, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: May 30th
2. Date the breach was discovered: June 10th
3. Describe the breach (provide sufficient detail, including cause):
   Provided the incorrect Abstract to customer by keying the wrong DL#. The individual was on his way to Alberta for work so he did not look at the Abstract to verify accuracy. When he got there he handed it to his employer. The employer held it and would not return it back to this individual.
4. Location of the breach:
   Marystown
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 1
6. Type(s) of individuals affected (check all that apply):
   - [x] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   Have requested retrieval of the document back to this office for shredding and offer to issue new DL # to person impacted by the breach,

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information: DL# and Driving record

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   The work area has safe in a secure location, the building has an alarm system and restricted access
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
   Only those who are authorized to print Driver abstracts or similar documents are permitted to do so. A procedure exist for issuance of driver abstract. We direct staff to check their
documents before handing them out to a customer. We will meet with employee and review this process.

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [ ] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

☐ Identity theft (higher risk if breach involves SIN # or financial information)
☐ physical harm or harassment (e.g. stalking)
☐ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
☐ financial cost
☐ loss of business or employment opportunities
☐ breach of contract and/or other legal obligations (e.g. from data loss)
☐ future breaches (technical failures)
☐ violation of professional standards or certificate standards
☐ risk to public health or safety
☒ Other (please specify): release of Driver information

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

☒ Yes  Date Analyst was notified: June 13, 2011
☐ No  When will the Analyst be notified?

14. Have law enforcement officials been notified?

☐ Yes  Who was notified and when?
☒ No  Will law enforcement be notified at a later time?

☐ Yes
☒ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?

☐ Yes  Who was notified and when?
☒ No

16. Have other authorities (E.g. professional bodies) been contacted?

☐ Yes  Who was notified and when?
☒ No  Will other authorities be notified at a later time?

☐ Yes
☐ No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckettt@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: June 24, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: May 19, 2011
2. Date the breach was discovered: June 23, 2011
3. Describe the breach (provide sufficient detail, including cause):
   The Motor Registration Division provided a customer with a photo identity card containing her picture but with tombstone data for a different person.
4. Location of the breach:
   Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   ☑ Client / Customer / Patient
   □ Employee
   □ Student
   □ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   The photo identity card was returned to MRD and will be destroyed when this ATIPP report is submitted. The client affected does not have a listed telephone number so will be contacted by mail as part of the letter of apology which will be sent today. She will be offered a new driver licence number.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, full address, driver's licence number, date of birth, gender, eye colour, and height

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   N/A
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
    All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to take due care in providing documents to customers at the counter. The clerk involved has been spoken with about this incident. All other clerks will be reminded the computer system
sometimes takes a bit of time to bring up the information on a customer and at times information on a previous customer is still on the system. A check of the data, beyond simply the first name, is necessary.

11. Describe the technical safeguards (access controls, audit controls, etc...) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   ☑ Identity theft (higher risk if breach involves SIN # or financial information)
   ☐ physical harm or harassment (e.g. stalking)
   ☐ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   ☐ financial cost
   ☐ loss of business or employment opportunities
   ☐ breach of contract and/or other legal obligations (e.g. from data loss)
   ☐ future breaches (technical failures)
   ☐ violation of professional standards or certificate standards
   ☐ risk to public health or safety
   ☐ Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   ☑ Yes Date Analyst was notified: June 24, 2011
   ☐ No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   ☐ Yes Who was notified and when?
   ☑ No Will law enforcement be notified at a later time?
   ☐ Yes
   ☑ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   ☐ Yes Who was notified and when?
   ☑ No

16. Have other authorities (E.g. professional bodies) been contacted?
   ☐ Yes Who was notified and when?
   ☑ No Will other authorities be notified at a later time?
   ☐ Yes
   ☑ No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

**IMPORTANT!** Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________
Signature of ATIPP Office Representative
If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: GOVERNMENT SERVICES

Division / Program: VITAL STATISTICS

Contact:

Name: KEN MULLALY
Title: REGISTRAR
Phone: 729-6340
Fax: 729-0946
E-Mail: kmullaly@gov.nl.ca
Mailing address: 5 Mews Place, P.O. BOX 8700 St. John's NL A1B 4J6

Date of Submission to the ATIPP Office: JULY 6, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: MAY 27, 2011
2. Date the breach was discovered: JULY 4, 2011
3. Describe the breach (provide sufficient detail, including cause):
   A birth certificate was sent out to the wrong address and when the client received the envelope they opened it and noticed it was for someone else and sealed the envelope back up and returned it to Vital Statistics.
4. Location of the breach:
   Government Service Center, Grand Falls-Windsor
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 1
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   Breached Information returned to Vital Statistics and the person whose birth certificate was inadvertently released to someone else has been advised of the error.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information:**
   Full Name, Date of Birth, Place of Birth, Parents Names, Registration Number and Date of Registration

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   We have locks on cabinets, alarm systems, sign in to office, door code
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
    proofreading, clean desk policy at days end.
11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:
☐ Encryption
☒ Password
☐ Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - ☒ Identity theft (higher risk if breach involves SIN # or financial information)
   - ☐ physical harm or harassment (e.g. stalking)
   - ☐ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - ☐ financial cost
   - ☐ loss of business or employment opportunities
   - ☐ breach of contract and/or other legal obligations (e.g. from data loss)
   - ☐ future breaches (technical failures)
   - ☐ violation of professional standards or certificate standards
   - ☐ risk to public health or safety
   - ☐ Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - ☐ Yes  Date Analyst was notified:
   - ☒ No  When will the Analyst be notified?  The ATIPP Coordinator for Government Services was notified on July 5, 2011 and will notify the Senior Privacy Analyst in the ATIPP office once receipt of this form.

14. Have law enforcement officials been notified?
   - ☐ Yes  Who was notified and when?
   - ☒ No  Will law enforcement be notified at a later time?
     - ☐ Yes
     - ☒ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - ☐ Yes  Who was notified and when?
   - ☒ No

16. Have other authorities (E.g. professional bodies) been contacted?
   - ☒ Yes  Who was notified and when?  Our Executive was notified on July 5, 2011
   - ☐ No  Will other authorities be notified at a later time?
     - ☐ Yes
     - ☐ No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

*IMPORTANT!* Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: HRLE

Division / Program: Income Support

Contact:

Name: Janelle Kenway
Title: PPDS
Phone: 709-729-7920
Fax: 
E-Mail: [REDACTED]
Mailing address: 3rd Floor, West Block, Confederation Building

Date of Submission to the ATIPP Office: July 21, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)

Employee incorrectly entered a personal email address. Should have been janellekenway@gov.nl.ca
- Office of Public Engagement
Risk Evaluation

Incident Description

1. Date the breach occurred: July 2011
2. Date the breach was discovered: July 19, 2011
3. Describe the breach (provide sufficient detail, including cause):
   At Metro Place (DPU), while compiling an applicant for a client in Western Region, 2 notices of overpayments for clients on the Avalon was included in the Western Applicant’s envelope. When the applicant sent back the application, the wrong documents were included with a note indicating these documents were not relevant to them.
4. Location of the breach: Metro Place - St. John's
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 3
6. Type(s) of individuals affected (check all that apply):
   □ Client / Customer / Patient
   □ Employee
   □ Student
   □ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   HRLE was unaware of the breach until the client sent back the wrong documents. We now have the documents and they are attached to the correct client file. Suggestions were made to provide either individual printers for workers or have less workers share the same printer to decrease the risk of documents becoming intermingled with wrong client files.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information:**
   Name, Address, Case Number, amount of overpayment

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   CSOs are very diligent in checking pages that are included in an application to prevent such a breach
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
N/A

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [ ] Encryption
- [ ] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

☐ Identity theft (higher risk if breach involves SIN # or financial information)
☐ physical harm or harassment (e.g. stalking)
☐ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
☐ financial cost
☐ loss of business or employment opportunities
☐ breach of contract and/or other legal obligations (e.g. from data loss)
☐ future breaches (technical failures)
☐ violation of professional standards or certificate standards
☐ risk to public health or safety
☒ Other (please specify): Department not being careful with records

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

☒ Yes Date Analyst was notified: July 19, 2011
☐ No When will the Analyst be notified?

14. Have law enforcement officials been notified?

☐ Yes Who was notified and when?
☒ No Will law enforcement be notified at a later time?
☐ Yes
☒ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?

☐ Yes Who was notified and when?
☒ No

16. Have other authorities (E.g. professional bodies) been contacted?

☐ Yes Who was notified and when?
☒ No Will other authorities be notified at a later time?
☐ Yes
☐ No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

______________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Justice

Division / Program: Provincial Court

Contact:

Name: Glenda Reid
Title: Court Manager
Phone: 709-729-6913
Fax: 709-729-2161
E-Mail: glendareid@provincial.court.nl.ca
Mailing address: Box 68, Atlantic Place, 215 Water Street, St. John’s, NL, A1C 6C9

Date of Submission to the ATIPP Office: July 29, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
**Risk Evaluation**

**Incident Description**

1. Date the breach occurred:  July 8, 2011
2. Date the breach was discovered: July 21, 2011
3. Describe the breach (provide sufficient detail, including cause):

   Complainant presented to traffic court office with Notice of Trial Date for Traffic Court letter addressed to another person. The envelope was addressed to him. Investigation revealed that his letter had been sent to the person identified on the letter he received. The only explanation is that it was the result of a clerical error when preparing the letters. The two letters were mixed up and inadvertently sent to the wrong people.

4. Location of the breach:

   Traffic Court

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 2

6. Type(s) of individuals affected (check all that apply):
   - [x] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):

   Complainant was asked to return the letter but wanted to keep it and meet with the manager to discuss further. The other person was contacted by telephone, notified of the breach and asked to return the incorrect letter by mail. She agreed to do so and did not express any concern. I met with the complainant on July 28. I apologized for the error; thanked him for bringing it to our attention; explained that I had followed up with the staff person involved and let him know that it was an unintentional error. I advised him of the formal complaint process; provided him with the required form; explained that I would also be reporting it. I asked that he return the letter not addressed to him and he agreed to include it with the complaint form. He wanted to know if I could do anything about his ticket. I explained that it was a completely separate issue that would not involve the OIPC. I provided contact information for him to speak with the Crown Attorney for Traffic Court.

**Personal Information Involved**

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information:**

   Name and Address.
Safeguards

9. Describe the **physical** safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   Copies are kept in office which is locked.

10. Describe the **administrative** safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:

   Procedures reviewed with staff and reminder of need for double checking the match of letter to envelope when sending correspondence.

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

   - Encryption
   - Password
   - Other (please specify): There is currently no automation in traffic court. Approximately 8000 tickets per month are processed using manual processes. Use of TRIM and other information technology would help to streamline processes, decrease workload, increase accuracy and make errors like this less likely in the future.
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - ☒ Identity theft (higher risk if breach involves SIN # or financial information)
   - ☐ physical harm or harassment (e.g. stalking)
   - ☐ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - ☐ financial cost
   - ☐ loss of business or employment opportunities
   - ☐ breach of contract and/or other legal obligations (e.g. from data loss)
   - ☐ future breaches (technical failures)
   - ☐ violation of professional standards or certificate standards
   - ☐ risk to public health or safety
   - ☒ Other (please specify): another person aware of traffic court appearance.

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - ☒ Yes  Date Analyst was notified: July 28, 2011
   - ☐ No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - ☐ Yes  Who was notified and when?
   - ☒ No  Will law enforcement be notified at a later time?
     - ☐ Yes
     - ☒ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - ☐ Yes  Who was notified and when?
   - ☒ No

16. Have other authorities (E.g. professional bodies) been contacted?
   - ☐ Yes  Who was notified and when?
   - ☒ No  Will other authorities be notified at a later time?
     - ☐ Yes
     - ☒ No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

**IMPORTANT!** Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: GOVERNMENT SERVICES

Division / Program: VITAL STATISTICS

Contact:

Name: KEN MULLALY
Title: REGISTRAR
Phone: 729-6340
Fax: 729-0946
E-Mail: kmullaly@gov.nl.ca
Mailing address: 5 Mews Place, P.O. BOX 8700 St. John's NL A1B 4J6

Date of Submission to the ATIPP Office: August 17, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: July 27, 2011
2. Date the breach was discovered: August 11, 2011
3. Describe the breach (provide sufficient detail, including cause):
   A birth certificate was sent out to the wrong address and when the client received the envelope they opened it and noticed it was for someone else and sealed the envelope back up and returned it to Vital Statistics.
4. Location of the breach:
   Government Service Center, Grand Falls-Windsor
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 1
6. Type(s) of individuals affected (check all that apply):
   - [x] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   Breached Information returned to Vital Statistics

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Full Name, Date of Birth, Place of Birth, Parents Names, Registration Number and Date of Registration

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   We have locks on cabinets, alarm systems, sign in to office, door code
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
    proofreading, clean desk policy at days end.
11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:
    - [ ] Encryption
Password

☐ Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

- ☒ Identity theft (higher risk if breach involves SIN # or financial information)
- ☐ physical harm or harassment (e.g. stalking)
- ☐ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
- ☐ financial cost
- ☐ loss of business or employment opportunities
- ☐ breach of contract and/or other legal obligations (e.g. from data loss)
- ☐ future breaches (technical failures)
- ☐ violation of professional standards or certificate standards
- ☐ risk to public health or safety
- ☐ Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
- ☒ Yes  Date Analyst was notified:  The ATIPP Coordinator for Government Services was notified on August 15, 2011 as was the Senior Privacy Analyst in the ATIPP office.
- ☐ No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
- ☐ Yes  Who was notified and when?
- ☒ No  Will law enforcement be notified at a later time?
  - ☐ Yes
  - ☒ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
- ☐ Yes  Who was notified and when?
- ☒ No

16. Have other authorities (E.g. professional bodies) been contacted?
- ☒ Yes  Who was notified and when?  Our Executive was notified on August 15, 2011
- ☐ No  Will other authorities be notified at a later time?
  - ☐ Yes
  - ☒ No
Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:
http://www.justice.gov.nl.ca/just/civil/atipp/

For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

_________________________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckettt@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: August 19, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred:  August 12, 2011
2. Date the breach was discovered:  August 17, 2011
3. Describe the breach (provide sufficient detail, including cause):
   The Motor Registration Division mailed a vehicle registration renewal and sticker to a customer. Included with these documents was a registration renewal and a sticker for a different individual.
4. Location of the breach:
   Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised):  One
6. Type(s) of individuals affected (check all that apply):
   ☒ Client / Customer / Patient
   ☐ Employee
   ☐ Student
   ☐ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   The vehicle registration and sticker mailed in error were returned to MRD and then mailed on to the correct owner. The client affected has been advised by telephone and is considering our offer to obtain a new driver licence number and a new licence plate for the car. A letter of apology will be sent today reiterating our offer for the client to obtain a new driver licence number and a new licence plate for the car.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history).  Do not include or send us the identifiable personal information:
   Name, full address, driver's licence number, Vehicle Plate Numbers, Sticker Number, Document Generation Date, Registration Expiry Date, Make/Model/Style/Colour/Mass/Year/Fuel of the vehicle, Vehicle Serial Number

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   N/A
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to take due care in mailings. MRD is exploring the option of changing the printing process for vehicle registrations to incorporate the sticker directly into the paper upon which the registration is printed. This will produce a single document which can be processed by the Transportation and Works mailroom for inserting into envelopes and mailing machine thereby eliminating the manual stapling of stickers to documents and the manual stuffing of envelopes.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [x] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

- Identity theft (higher risk if breach involves SIN # or financial information)
- Physical harm or harassment (e.g. stalking)
- Emotional harm, humiliation or damage to reputation (e.g. disclosure of mental health records)
- Financial cost
- Loss of business or employment opportunities
- Breach of contract and/or other legal obligations (e.g. from data loss)
- Future breaches (technical failures)
- Violation of professional standards or certificate standards
- Risk to public health or safety
- Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

- Yes  Date Analyst was notified: August 19, 2011
- No  When will the Analyst be notified?

14. Have law enforcement officials been notified?

- Yes  Who was notified and when?
- No  Will law enforcement be notified at a later time?
  - Yes
  - No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?

- Yes  Who was notified and when?
- No

16. Have other authorities (E.g. professional bodies) been contacted?

- Yes  Who was notified and when?
- No  Will other authorities be notified at a later time?
  - Yes
  - No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

______________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Public Service Commission
Division / Program: Strategic Scheduling
Contact:
Name: Rawlene Thomas
Title: Director, AoI
Phone: 8581
Fax: 6234
E-Mail: rawlene.thomas@gov.nl.ca
Mailing address:

Date of Submission to the ATIPP Office: April 28, 2011.

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: August 25, 2011
2. Date the breach was discovered: August 25, 2011
3. Describe the breach (provide sufficient detail, including cause): Applicants' email addresses accidentally shared with other applicants
4. Location of the breach: P.O. Box 1000, St. John's, NF
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 6
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   Electronic message recall attempted, not successful.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name.

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   Not applicable.
10. Describe the administrative safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:
    Regular email practice requires use of BCC when notifying applicants via email
11. Describe the technical safeguards (access controls, audit controls, etc...) currently in place to protect the personal information in your custody and control:
   - Encryption
   - Password
   - Other (please specify): Confidentiality requirements associated with position.
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [ ] Identify theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [x] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records) Knowledge of applicant only.
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes Date Analyst was notified: Upon return from leave
   - [ ] No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes Who was notified and when?
   - [x] No Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes Who was notified and when?
   - [x] No Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/

Note: All individuals contacted, breach explained, apology offered.
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Robert Groves
Title: Manager
Phone: 709-466-4064
Fax: 709-466-4070
E-Mail: rgroves@gov.nl.ca
Mailing address: 8 Myer's Avenue, Suite 201, Clarenville, NL A5A 1T5

Date of Submission to the ATIPP Office: 2011 08 30

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: August 23, 2011
2. Date the breach was discovered: August 25, 2011
3. Describe the breach (provide sufficient detail, including cause):
   Drivers Licence was put in envelop with another persons address, in error, and mailed to wrong person.
4. Location of the breach:
   Clarenville - GSC
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   The drivers licence has been returned to the office, recovered and destroyed. We are in the process of advising the client by mail and will attempt to contact her by phone. The client who was impacted by the breach, has been offered the option to obtain a new driver's licence number.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Drivers Licence Number

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   The work area has a safe, alarm system and has restricted access
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
    All staff have completed the on-line protection of privacy training and area aware of the importance of protecting a persons personal information
11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [ ] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - ☐ Identity theft (higher risk if breach involves SIN # or financial information)
   - ☐ Physical harm or harassment (e.g. stalking)
   - ☐ Emotional harm, humiliation or damage to reputation (e.g. disclosure of mental health records)
   - ☐ Financial cost
   - ☐ Loss of business or employment opportunities
   - ☐ Breach of contract and/or other legal obligations (e.g. from data loss)
   - ☐ Future breaches (technical failures)
   - ☐ Violation of professional standards or certificate standards
   - ☐ Risk to public health or safety
   - ☑ Other (please specify): Drivers licence information released to wrong person

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - ☑ Yes Date Analyst was notified: August 30, 2011
   - ☐ No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - ☐ Yes Who was notified and when?
   - ☑ No Will law enforcement be notified at a later time?
     - ☐ Yes
     - ☑ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - ☐ Yes Who was notified and when?
   - ☑ No

16. Have other authorities (e.g. professional bodies) been contacted?
   - ☐ Yes Who was notified and when?
   - ☑ No Will other authorities be notified at a later time?
     - ☐ Yes
     - ☑ No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

______________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Eastern School District

Division / Program: Villanova Junior High

Contact:

Name: Dr. Albert Trask
Title: Assistant Director of Education, Rural Education and Corporate Services
Phone: 758-2341
Fax: 758-2706
E-Mail: alberttrask@esdnl.ca
Mailing address: Suite 601 Atlantic Place, 215 Water St. St. John's A1C6C9

Date of Submission to the ATIPP Office: September 14, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
**Risk Evaluation**

**Incident Description**

1. Date the breach occurred: September 14, 2011
2. Date the breach was discovered: September 14, 2011
3. Describe the breach (provide sufficient detail, including cause):
   
   A fax was sent to an incorrect fax number which included the child’s name, address, parents names, date of birth, MCP number, phone number as well as sensitive information regarding the child’s educational assessments. The recipient that received the fax in error has been contacted and the information has been shredded.

4. Location of the breach:
   
   Villanova Junior High, CBS, NL

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): one student

6. Type(s) of individuals affected (check all that apply):
   
   - [ ] Client / Customer / Patient
   - [ ] Employee
   - [X] Student
   - [ ] Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):

   Recipient was contacted and we have confirmed all information has been shredded.

**Personal Information Involved**

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:

   child’s name, address, parents names, date of birth, MCP number, phone number as well as sensitive information regarding the child’s educational assessments

**Safeguards**

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   human error, staff told to be more careful

10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:

    Only those who need access to information have it. All personal information in paper format is stored in locked cabinets or rooms, electronic files are stored on password protected servers at each school.
11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [ ] Encryption
- [ ] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [ ] Identify theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [ ] Yes  Date Analyst was notified: September 14, 2011
   - [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [ ] No  Will law enforcement be notified at a later time?
     - [ ] Yes
     - [ ] No

15. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?  Parents of the student was notified by letter September 14
   - [ ] No  Will other authorities be notified at a later time?
     - [ ] Yes
     - [ ] No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckett@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: September 19, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: about September 12, 2011
2. Date the breach was discovered: September 19, 2011
3. Describe the breach (provide sufficient detail, including cause):
   The Motor Registration Division mailed a vehicle registration renewal and sticker to a customer. Included with these documents was a registration renewal and a sticker for a different individual.
4. Location of the breach:
   Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient  
   - Employee  
   - Student  
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   The vehicle registration and sticker mailed in error will be returned to MRD and then mailed on to the correct owner. The client affected will be advised by telephone or mail and will be offered the opportunity to obtain a new driver licence number and/or a new licence plate for the car. A letter of apology will be sent reiterating our offer for the client to obtain a new driver licence number and a new licence plate for the car.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, full address, driver's licence number, Vehicle Plate Numbers, Sticker Number, Document Generation Date, Registration Expiry Date, Make/Model/Style/Colour/Mass/Year/Fuel of the vehicle, Vehicle Serial Number

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   N/A
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to take due care in mailings. MRD is exploring the option of changing the printing process for vehicle registrations to incorporate the sticker directly into the paper upon which the registration is printed. This will produce a single document which can be processed by the Transportation and Works mailroom for inserting into envelopes and mailing machine thereby eliminating the manual stapling of stickers to documents and the manual stuffing of envelopes.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [ ] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] Physical harm or harassment (e.g. stalking)
   - [ ] Emotional harm, humiliation or damage to reputation (e.g. disclosure of mental health records)
   - [ ] Financial cost
   - [ ] Loss of business or employment opportunities
   - [ ] Breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] Future breaches (technical failures)
   - [ ] Violation of professional standards or certificate standards
   - [ ] Risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [ ] Yes Date Analyst was notified: August 19, 2011
   - [ ] No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes Who was notified and when?
   - [ ] No Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes Who was notified and when?
   - [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes Who was notified and when?
   - [x] No Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For **Internal Use by the ATIPP Office Only**

Date Reporting form received by the ATIPP Office:

*IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.*

**Received by:**

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body:  Government Services

Division / Program:  Motor Registration Division

Contact:

Name:  Tom Beckett
Title:  Deputy Registrar
Phone:  729-2520
Fax:  729-6955
E-Mail:  beckettt@gov.nl.ca
Mailing address:  P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office:  September 20, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
**Risk Evaluation**

**Incident Description**

1. Date the breach occurred:  September 14, 2011
2. Date the breach was discovered:  September 19, 2011
3. Describe the breach (provide sufficient detail, including cause):
   
   The Motor Registration Division mailed a medical suspension to an individual with substantially the same name as the person to whom the suspension should have gone. This occurred as the birth year and the first and last names of both individuals was the same.

4. Location of the breach:
   
   Mount Pearl

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised):  One

6. Type(s) of individuals affected (check all that apply):
   
   - [x] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   
   The person to whom the information was sent has received verbal apologies from the staff and from the registrar. A letter of apology will also be sent. The person whose personal information was released in error will receive a verbal apology followed by a written apology.

**Personal Information Involved**

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history).  
   
   Do not include or send us the identifiable personal information:

   Partial Name, indication of a medical suspension on the driver licence, requirement for a routine medical, requirement for an update on cognitive status, requirement to undertake an occupational therapy driving assessment

**Safeguards**

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   N/A

10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to take due care in mailings. Staff have been directed to be thorough in checking full birth date to include year, month, and day when assigning medical files such that the file is assigned to the correct person.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [x] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

- Identity theft (higher risk if breach involves SIN # or financial information)
- Physical harm or harassment (e.g. stalking)
- Emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
- Financial cost
- Loss of business or employment opportunities
- Breach of contract and/or other legal obligations (e.g. from data loss)
- Future breaches (technical failures)
- Violation of professional standards or certificate standards
- Risk to public health or safety
- Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

- Yes Date Analyst was notified: September 20, 2011
- No When will the Analyst be notified?

14. Have law enforcement officials been notified?

- Yes Who was notified and when?
- No Will law enforcement be notified at a later time?

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?

- Yes Who was notified and when?
- No

16. Have other authorities (E.g. professional bodies) been contacted?

- Yes Who was notified and when?
- No Will other authorities be notified at a later time?

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

**IMPORTANT!** Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

**Received by:**

_____________________
Signature of ATIPP Office Representative
If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Government Service Centre (Motor Registration Division)

Contact:

Name: Robert Groves, Manager of Operations
Title: Manager
Phone: 709-466-4064
Fax: 709-466-4070
E-Mail: rgroves@gov.nl.ca
Mailing address: 8 Myer's Avenue, Suite 201, Clarenville, NL A5A 1T5

Date of Submission to the ATIPP Office: 2011 09 23

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: September 21st, 2011
2. Date the breach was discovered: September 22nd, 2011
3. Describe the breach (provide sufficient detail, including cause):
   Wrong Driver's Licence Number was keyed in error while processing a vehicle transfer and
given to wrong customer. Keyed letter M instead of V at beginning of driver's licence
number. The number keyed was an inactive NL Driver's licence number.
4. Location of the breach:
   Marystown - GSC
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal
   information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of
   breached information; replacement of locks; shut down of IT systems, etc…):
   The registration has been returned to the office, recovered and destroyed. We are in the
   process of advising the client by mail and will attempt to contact him by phone.
The client who was impacted by the breach, will be offered the option to obtain a
new driver's licence number should he return to NL.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information
   or medical history). Do not include or send us the identifiable personal information:
   Inactive Drivers Licence Number

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect
   the personal information in your custody and control:
   The work area has a safe, alarm system and has restricted access
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to
    protect the personal information in your custody and control:
    All staff have completed the on-line protection of privacy training and area aware of the
    importance of protecting a persons personal information
11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [ ] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [x] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [x] Other (please specify): Inactive Drivers licence information released to wrong person

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [ ] Yes Date Analyst was notified:
   - [ ] No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes Who was notified and when?
   - [x] No Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes Who was notified and when?
   - [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes Who was notified and when?
   - [x] No Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

**Contact Information**

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Carolyn Burggraaf  
Title: Registrar of Motor Vehicles  
Phone: 729-4175  
Fax: 729-6955  
E-Mail: cburggra@gov.nl.ca  
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: September 27, 2011

*(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)*
Risk Evaluation

Incident Description

1. Date the breach occurred: September 23, 2011
2. Date the breach was discovered: September 25, 2011
3. Describe the breach (provide sufficient detail, including cause):
   [Redacted]

4. Location of the breach:
   St. John's, NL
5. Estimated number of individuals directly affected by the privacy breach (i.e., whose personal information has been compromised): None
6. Type(s) of individuals affected (check all that apply):
   □ Client / Customer / Patient
   □ Employee
   □ Student
   □ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g., retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   The OCIO was notified by the Registrar of Motor Vehicles of the theft.

Personal Information Involved

8. Describe the personal information involved (e.g., name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   At this time, no personal information identified as being contained on laptop.

Safeguards

9. Describe the physical safeguards (e.g., locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   N/A
10. Describe the administrative safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:
    N/A
11. Describe the technical safeguards (access controls, audit controls, etc...) currently in place to protect the personal information in your custody and control:
- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

☐ Identity theft (higher risk if breach involves SIN # or financial information)
☐ physical harm or harassment (e.g. stalking)
☐ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
☐ financial cost
☐ loss of business or employment opportunities
☐ breach of contract and/or other legal obligations (e.g. from data loss)
☐ future breaches (technical failures)
☐ violation of professional standards or certificate standards
☐ risk to public health or safety
☐ Other (please specify): None at this time

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   ☑ Yes Date Analyst was notified: September 26, 2011
   ☐ No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   ☑ Yes Who was notified and when? The Royal Newfoundland Constabulary - September 23, 2011
   ☐ No Will law enforcement be notified at a later time?
      ☑ Yes
      ☐ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   ☐ Yes Who was notified and when?
   ☑ No

16. Have other authorities (E.g. professional bodies) been contacted?
   ☐ Yes Who was notified and when?
   ☑ No Will other authorities be notified at a later time?
      ☑ Yes
      ☐ No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:
http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division, Mount Pearl

Contact:

Name: Debby Power
Title: Manager of Business Practices
Phone: 729-4953
Fax: 729-6955
E-Mail: DAPower@gov.nl.ca
Mailing address: PO Box 8710, St John's NL A1B 4J5

Date of Submission to the ATIPP Office: October 5, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: June 6, 2011
2. Date the breach was discovered: October 3, 2011
3. Describe the breach (provide sufficient detail, including cause):
   A customer was at the counter to transfer a vehicle & pay applicable tax. The wrong drivers licence number was keyed on the MRD system resulting in the customer receiving a vehicle registration & tax receipt in another person's name. The cause of the breach was a clerical keying error.
4. Location of the breach:
   Motor Registration Division, Mount Pearl front counter
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 1
6. Type(s) of individuals affected (check all that apply):
   ☒ Client / Customer / Patient
   ☐ Employee
   ☐ Student
   ☐ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   The customer has been asked to return the documents to the MRD office and the vehicle record information has been corrected on the system with the correct customers drivers licence number.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, address, drivers licence number, vehicle plate and serial number.

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   Secure system with password protection.
10. Describe the administrative safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:
   All staff have received ATIPP training, both online & in person at MRD Mt Pearl. Staff have been directed to cross check documents before handing to customers to ensure the correct information has been keyed,
11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [x] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes  Date Analyst was notified:  October 5, 2011
   - [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will law enforcement be notified at a later time?
   - [ ] Yes
   - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes  Who was notified and when?
   - [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will other authorities be notified at a later time?
   - [ ] Yes
   - [x] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckettt@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: October 5, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: about September 23, 2011
2. Date the breach was discovered: October 4, 2011
3. Describe the breach (provide sufficient detail, including cause):
   The Motor Registration Division generated a new driver licence following a successful road test. Inadvertently, the alpha character on the carrier form for the driver licence had an P transposed for an R with the result the driver licence was mailed to the wrong person.
4. Location of the breach: Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   The father of the individual who received the driver licence in error returned the licence to MRD. The individual whose privacy was breached will be contacted as to their desire for a new driver licence number. The driver licence has now been mailed to the correct address. A standard letter advising of the privacy breach and offering a new driver licence number will be sent to the individual affected.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, driver's licence number, photo, driver class, date of birth, gender, eye colour, height, date of first licence, signature

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   N/A
10. Describe the administrative safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to cross check information given out. Meetings with staff were held on January 14, 2011, to emphasize the need for due care in mailings.

On February 15, 2011, a meeting was held with Registrar of Motor Vehicles and Counter Supervisor to discuss the importance of checking name on cards against name on mail out. In addition to current practice of a senior clerk being responsible for mailing driver licences, the clerk will be required to log mail outs so if any errors occur corrective action will be taken.

Two clerks have been identified as having responsibility for the mailing of the batch of driver licences including the one sent in error. The Supervisor discussed this situation with both clerks.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [x] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes  Date Analyst was notified: October 5, 2011
   - [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [ ] No  Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes  Who was notified and when?
   - [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

_________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Justice

Division / Program: Victim Services, Corrections and Community Services

Contact:

   Name: Anita Stanley
   Title: A/Provincial Manager
   Phone: 792.0885
   Fax: 729.5100
   E-Mail: anitastanley@gov.nl.ca
   Mailing address: 4th Floor, Confederation Bldg, East Block
                   P.O. Box 8700, St. John's NL A1B 4J6

Date of Submission to the ATIPP Office: October 5, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: on or about September 22, 2011
2. Date the breach was discovered: September 22, 2011
3. Describe the breach (provide sufficient detail, including cause):

A letter and information package was forwarded to a client, after the Victim Services Regional Coordinator made contact with the client. The letter detailed the nature of the alleged incident as well as the referral source. The letter was received by an unintended recipient and that individual opened the letter. The individual allegedly opened the letter because it was addressed with her maiden name and her daughter’s first name. She contacted her adult daughter who then contacted the Victim Services Regional Coordinator on September 22, 2011 to advise of the mistake.

A review of this matter discovered that the envelop was addressed with the client’s correct last name but the wrong given name. The address was correct but given its general nature (i.e., [redacted]), it was not sufficient to prevent the mail from being delivered to an unintended recipient.

4. Location of the breach:

[redacted] s.30(1)

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): two

6. Type(s) of individuals affected (check all that apply):
   - ☒ Client / Customer / Patient
   - ☐ Employee
   - ☐ Student
   - ☒ Other (please specify): Nurse - referral source

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):

1. The client was notified of the breach
2. The daughter of the unintended recipient of the letter was advised of the sensitive nature of the information and the importance of maintaining an individual’s private and confidential information and not sharing that information with anyone else
3. The client’s mother decided to retrieve the letter from the unintended recipient
4. There have been repeated attempts made to contact the referral source (although no contact has been made to date) to advise of the breach

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:

1. The client’s personal information included:
- name
- address
- nature of incident
- status of investigation
- request for services from the Victim Services Program

2. The personal information of the referral source included:
- name
- occupation
- work site

However, it is arguable whether the information relating to the referral source is personal information given that this person works for a public body.

**Safeguards**

9. Describe the **physical** safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   The Victim Services Division has numerous safeguards which protect personal information including:
   - locked filing cabinets
   - locked offices
   - locked building at the end of the work day
   - alarm systems in some offices

   It is noted that this is the first privacy breach for the Victim Services Division since proclamation of Part IV of the ATIPPA which resulted directly from human error. A review of practices and procedures will be conducted with a view to minimizing chances of future privacy breaches.

10. Describe the **administrative** safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:

    As a result of this breach, Victim Services will be reviewing its practices to minimize the impact of a privacy breach. For example, personal details in client letters will be kept to a minimum.

    Administrative safeguards include:
    - use of file numbers instead of clients' names in emails, internal correspondence

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

    - Encryption
    - Password
    - Other (please specify):  file audits
Potential Harm
12. Identify any harm that may result from the breach (check all that apply):
   - [ ] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [x] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification
13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes Date Analyst was notified: September 27, 2011
   - [ ] No When will the Analyst be notified?
14. Have law enforcement officials been notified?
   - [ ] Yes Who was notified and when?
   - [x] No Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No
15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [x] Yes Who was notified and when? Steve Ring, September 23, 2011
   - [ ] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes Who was notified and when?
   - [x] No Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

*IMPORTANT!* Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
# Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the *Access to Information and Protection of Privacy (ATIPP) Act*.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

## Contact Information

**Department / Public Body:** Government Services  

**Division / Program:** Motor Registration Division

**Contact:**

Name: Tom Beckett  
Title: Deputy Registrar  
Phone: 729-2520  
Fax: 729-6955  
E-Mail: beckettt@gov.nl.ca  
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

**Date of Submission to the ATIPP Office:** October 6, 2011

*(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)*
Risk Evaluation

Incident Description

1. Date the breach occurred: about September 28, 2011
2. Date the breach was discovered: October 5, 2011
3. Describe the breach (provide sufficient detail, including cause):
   The Motor Registration Division generated a new driver licence following a successful road test. Inadvertently, the alpha character on the carrier form for the driver licence had an C transposed for an O with the result the driver licence was mailed to the wrong person.
4. Location of the breach:
   Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   The mother of the individual who received the driver licence in error returned the licence to MRD. The individual whose privacy was contacted and declined the offer of our generating a new driver licence number. The driver licence has now been mailed to the correct address. A standard letter advising of the privacy breach and again offering a new driver licence number will be sent to the individual affected.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, driver's licence number, photo, driver class, date of birth, gender, eye colour, height, date of first licence, signature

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   N/A
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to cross check information given out. Meetings with staff were held on January 14, 2011, to emphasize the need for due care in mailings.

On February 15, 2011, a meeting was held with Registrar of Motor Vehicles and Counter Supervisor to discuss the importance of checking name on cards against name on mail out. In addition to current practice of a senior clerk being responsible for mailing driver licences, the clerk will be required to log mail outs so if any errors occur corrective action will be taken.

Two clerks have been identified as having responsibility for the mailing of the batch of driver licences including the one sent in error. The Supervisor discussed this situation with both clerks. In addition, the Supervisor is in the process of one-on-one discussions with each senior clerk to reinforce the serious nature of security of personal information.

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [x] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm
12. Identify any harm that may result from the breach (check all that apply):
   - [x] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification
13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes  Date Analyst was notified: October 6, 2011
   - [ ] No  When will the Analyst be notified?
14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No
15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes  Who was notified and when?
   - [x] No
16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

**IMPORTANT!** Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckettt@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: October 17, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
**Risk Evaluation**

**Incident Description**

1. Date the breach occurred: June 9, 2011
2. Date the breach was discovered: October 13, 2011
3. Describe the breach (provide sufficient detail, including cause):
   
   A clerk at the Motor Registration Division front counter in Mount Pearl keyed a driver licence supplied on an application for transfer of a vehicle and generated the registration document. The driver licence number provided was incorrect resulting in the vehicle registration information for a different individual being provided to the person at the counter.

4. Location of the breach: Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):

   The customer who received the incorrect registration has been provided with the correct registration for his vehicle. The client whose information was released has been advised by telephone and accepted our offer to obtain a new driver licence number. A letter of apology will be sent today.

**Personal Information Involved**

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information:**

   Name, full address, and driver's licence number

**Safeguards**

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   , N/A

10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to take due care in serving customers. The clerk who provided the wrong registration form has been spoken with so as to ensure additional care in passing out information.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [x] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [x] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes  Date Analyst was notified: October 17, 2011
   - [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [x] Yes  Who was notified and when?
   - [ ] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckett@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: October 20, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
**Risk Evaluation**

**Incident Description**

1. Date the breach occurred: about September 27, 2011

2. Date the breach was discovered: October 17, 2011

3. Describe the breach (provide sufficient detail, including cause):
   
   The Motor Registration Division mailed a revised vehicle registration to a customer. Included with this document was a registration renewal and a sticker for a different individual.

4. Location of the breach:
   
   Mount Pearl

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One

6. Type(s) of individuals affected (check all that apply):
   
   - [x] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   
   The vehicle registration and sticker mailed in error has been returned to MRD. A replacement registration and sticker have already been mailed on to the correct owner. The client affected could not be contacted by telephone. They will be advised by mail and will be offered the opportunity to obtain a new driver licence number and/or a new licence plate for the car. This letter will include an apology for the breach.

**Personal Information Involved**

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information:**
   
   Name, full address, driver's licence number, Vehicle Plate Numbers, Sticker Number, Document Generation Date, Registration Expiry Date, Make/Model/Style/Colour/Mass/Year/Fuel of the vehicle, Vehicle Serial Number

**Safeguards**

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   
   N/A

10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to take due care in mailings. MRD is exploring the option of changing the printing process for vehicle registrations to incorporate the sticker directly into the paper upon which the registration is printed. This will produce a single document which can be processed by the Transportation and Works mailroom for inserting into envelopes and mailing machine thereby eliminating the manual stapling of stickers to documents and the manual stuffing of envelopes.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

- Identity theft (higher risk if breach involves SIN # or financial information)
- Physical harm or harassment (e.g. stalking)
- Emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
- Financial cost
- Loss of business or employment opportunities
- Breach of contract and/or other legal obligations (e.g. from data loss)
- Future breaches (technical failures)
- Violation of professional standards or certificate standards
- Risk to public health or safety
- Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

- Yes Date Analyst was notified: October 20, 2011
- No When will the Analyst be notified?

14. Have law enforcement officials been notified?

- Yes Who was notified and when?

- No Will law enforcement be notified at a later time?

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?

- Yes Who was notified and when?
- No

16. Have other authorities (E.g. professional bodies) been contacted?

- Yes Who was notified and when?

- No Will other authorities be notified at a later time?

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

**IMPORTANT!** Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Education

Division / Program: Information Management & Special Projects

Contact:

Name: Brian Evans
Title: Director, IM & Special Projects
Phone: 729-1841
Fax: 729-3462
E-Mail: brianevans@gov.nl.ca
Mailing address: P.O. Box 8700, 3rd Floor, West Block, Confederation Bldg, St. John’s, NL, A1B 4J6

Date of Submission to the ATIPP Office: October 24, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: October 21, 2011
2. Date the breach was discovered: October 21, 2011
3. Describe the breach (provide sufficient detail, including cause):
   There was an inadvertent disclosure of an unredacted document to an ATIPPA Applicant. The Department has been involved in a review with the Office of the Information and Privacy Commissioner pursuant to a document requested by an applicant. The OIPC provided a recommendation to release additional information to the Applicant. On October 21, 2011, the Department intended to release another copy of the document to the applicant with additional information disclosed. However, the department's ATIPP Coordinator mistakenly e-mailed the audited version of the document to the applicant, not the redacted version.
4. Location of the breach:
   Department of Education
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): one
6. Type(s) of individuals affected (check all that apply):
   - [ ] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [x] Other (please specify): ex-employee of CNA
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   Upon discovery of the breach, the department's ATIPPA Coordinator immediately sent notification to the applicant requesting i) confirmation that any record of the content of the unredacted document sent by mistake has been deleted; ii) stating the unredacted document contains protected personal information of identifiable individuals; and iii) no further dissemination of any protected personal information or other redacted material.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information:**
   The personal information involved includes i) information about an individual who, although not named, is likely identifiable (by office, small group) and ii) opinion by a person about an individual, where although the individual is not named, in the context is identifiable by someone with knowledge of the work environment.
Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   n/a

10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
    n/a

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

   - Encryption
   - Password
   - ☑ Other (please specify): n/a
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [ ] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] Physical harm or harassment (e.g. stalking)
   - [x] Emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] Financial cost
   - [ ] Loss of business or employment opportunities
   - [ ] Breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] Future breaches (technical failures)
   - [ ] Violation of professional standards or certificate standards
   - [ ] Risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes  Date Analyst was notified: October 21, 2011 directly to Director, ATIPP Office
   - [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [x] Yes  Who was notified and when?  Anne Marie Rose, October 21, 2011
   - [ ] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

______________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Carolyn Burggraaf
Title: Registrar of Motor Vehicles
Phone: 729-7333
Fax: 729-6955
E-Mail: cburggra@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: October 26, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: October 25, 2011
2. Date the breach was discovered: October 25, 2011
3. Describe the breach (provide sufficient detail, including cause):

   The Motor Registration Division received an email from a client which included her name, credit card number and card expiry date requesting payment of a parking ticket. In error the respondent forwarded the client's email to all Staff Department of Justice - Atlantic Place, rather than the appropriate contact within Fines Administration, Department of Justice (approximately 150 Department of Justice employees) for response to the client.

4. Location of the breach:

   Mount Pearl

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One

6. Type(s) of individuals affected (check all that apply):

   ☑ Client / Customer / Patient
   ☐ Employee
   ☐ Student
   ☐ Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):

   The client was contacted by email and telephone by the Registrar of Motor Vehicles with an apology and a recommendation to cancel her credit card. In addition a retraction of the email sent in error was sent to minimize the repercussions or potential misuse of the credit card. In addition, a separate email was sent outlining the issue and requesting the previous email, which had been sent in error, be deleted. A letter of apology to the client will also be sent.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:

   Email address, name, credit card type, credit card number and card expiry date

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   N/A

10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to take due care in email, mailing, and face-to-face service. Tip sheets on handling of personal information have been posted throughout the office.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
- [x] Identity theft (higher risk if breach involves SIN # or financial information)
- [ ] physical harm or harassment (e.g. stalking)
- [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
- [x] financial cost
- [ ] loss of business or employment opportunities
- [ ] breach of contract and/or other legal obligations (e.g. from data loss)
- [ ] future breaches (technical failures)
- [ ] violation of professional standards or certificate standards
- [ ] risk to public health or safety
- [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
- [x] Yes Date Analyst was notified: October 25, 2011
- [ ] No When will the Analyst be notified?

14. Have law enforcement officials been notified?
- [ ] Yes Who was notified and when?
- [x] No Will law enforcement be notified at a later time?
  - [ ] Yes
  - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
- [ ] Yes Who was notified and when?
- [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
- [ ] Yes Who was notified and when?
- [x] No Will other authorities be notified at a later time?
  - [ ] Yes
  - [x] No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:
http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Government Services

Division / Program: Motor Registration Division

Contact:

Name: Tom Beckett
Title: Deputy Registrar
Phone: 729-2520
Fax: 729-6955
E-Mail: beckett@gov.nl.ca
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office: November 21, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
**Risk Evaluation**

**Incident Description**

1. Date the breach occurred: November 9, 2011
2. Date the breach was discovered: November 17, 2011
3. Describe the breach (provide sufficient detail, including cause):
   
   The Motor Registration Division generated a new driver licence based on an e-mail request. Inadvertently, the alpha character for the driver licence had an B transposed for a W on the MRD system with the result the driver licence of a different person was changed and mailed to the person requesting the change of address. This person then opened the letter.

4. Location of the breach: Mount Pearl

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One

6. Type(s) of individuals affected (check all that apply):
   
   - [x] Client / Customer / Patient
   - [ ] Employee
   - [ ] Student
   - [ ] Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):

   The wife of the individual who received the driver licence in error returned the licence to MRD. The individual whose privacy was affected will be contacted and offered the opportunity of our generating a new driver licence number. The address on their driver licence has been changed back to the correct address. A standard letter advising of the privacy breach and again offering a new driver licence number will be sent to the individual affected. The driver licence of the individual requesting the change has been correctly changed.

**Personal Information Involved**

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). **Do not include or send us the identifiable personal information:**

   Name, driver's licence number, restriction to corrective lenses, photo, driver class, date of birth, gender, eye colour, height, date of first licence, signature

**Safeguards**

9. Describe the **physical** safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   N/A
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:

All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to cross check information given out. Meetings with staff were held on January 14, 2011, to emphasize the need for due care in mailings. Ongoing reminders have been issued and spoken about the sensitivity of information.

The Supervisor of processing held one-on-one discussions with each senior clerk to reinforce the serious nature of security of personal information. The clerk who mis-keyed the change of address was spoken to directly on this matter.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

- Identity theft (higher risk if breach involves SIN # or financial information)
- Physical harm or harassment (e.g. stalking)
- Emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
- Financial cost
- Loss of business or employment opportunities
- Breach of contract and/or other legal obligations (e.g. from data loss)
- Future breaches (technical failures)
- Violation of professional standards or certificate standards
- Risk to public health or safety
- Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

- Yes  Date Analyst was notified: November 21, 2011
- No  When will the Analyst be notified?

14. Have law enforcement officials been notified?

- Yes  Who was notified and when?
- No  Will law enforcement be notified at a later time?

- Yes
- No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?

- Yes  Who was notified and when?
- No

16. Have other authorities (E.g. professional bodies) been contacted?

- Yes  Who was notified and when?
- No  Will other authorities be notified at a later time?

- Yes
- No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

______________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: College of the North Atlantic - Qatar

Division / Program: Human Resources

Contact:

Name: Shawn Brace
Title: Vice President - Finance and Administration
Phone: +974 4495 2057
Fax: +974 4495 2054
E-Mail: shawn.brace@cna-qatar.edu.qa
Mailing address: P.O. Box: 24449; Doha - Qatar

Date of Submission to the ATIPP Office: November 24, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: October 27, 2011
2. Date the breach was discovered: November 21, 2011
3. Describe the breach (provide sufficient detail, including cause):
   A document posted to our HR Intranet site contained information regarding individual employees and their respective salaries and their Dates of Birth. The document was developed specifically for the purpose of Workers Compensation and Life Insurance. We have been made aware that a number of employees have downloaded this document and have circulated it amongst other employees.
4. Location of the breach:
   CNA-Qatar, Doha, Qatar
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 600
6. Type(s) of individuals affected (check all that apply):
   [ ] Client / Customer / Patient
   [x] Employee
   [ ] Student
   [ ] Other (please specify): Approximately 25 other employees of
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc.):
   The document has been removed from the intranet. Communication has sent to all of our employees regarding the circulation of confidential information and specifically referencing the return of the document to HR and directing no further circulation of this document.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, Salary Information and Birth Date, Nationality and Employee number.

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   Locks, alarms and security cameras.
10. Describe the administrative safeguards (policies, procedures, etc. . .) currently in place to protect the personal information in your custody and control:
Limited HR employee access by role to post information to the intranet and sharepoint.

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [ ] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

- [ ] Identity theft (higher risk if breach involves SIN # or financial information)
- [ ] Physical harm or harassment (e.g. stalking)
- [x] Emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
- [ ] Financial cost
- [ ] Loss of business or employment opportunities
- [x] Breach of contract and/or other legal obligations (e.g. from data loss)
- [ ] Future breaches (technical failures)
- [ ] Violation of professional standards or certificate standards
- [ ] Risk to public health or safety
- [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

- [ ] Yes  Date Analyst was notified: 
- [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?

- [ ] Yes  Who was notified and when?
- [x] No  Will law enforcement be notified at a later time?

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?

- [ ] Yes  Who was notified and when?
- [x] No

16. Have other authorities (E.g. professional bodies) been contacted?

- [ ] Yes  Who was notified and when?
- [x] No  Will other authorities be notified at a later time?

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

______________________________
Signature of ATIPP Office Representative
Privacy Breach Report Form

Date of Submission to the ATIPP Office: December 1, 2011
Please indicate the date the Privacy Breach Report form is completed, not the date on which the privacy breach occurred.

Contact Information (for the person who can answer questions about the breach if necessary)

Department / Public Body: Service NL
Division / Program: Motor Registration Division

Contact Details

Name: Carolyn Burggraaf
Title: Registrar of Motor Vehicles
Phone: 729-7333
Fax: 729-6955
Email: cburggra@gov.nl.ca
Mailing Address: MRD - Mt. Pearl

Risk Evaluation

Incident Description

Date the breach occurred: Dec. 2010-Oct. 2011
Length of time breach occurred (if more exceeds 1 day): various days throughout 10 mths
Date the breach was discovered: reported to HR Oct. 24/11. Audit was run on Oct. 26/11.
Location of the breach: MRD system

A [redacted] received a notice of traffic fines in the mail. His name was attached but the licence plate # on the letter wasn’t his. Instead of calling MRD right away to notify them of the error, he made the inquiry himself at work to verify who the licence plate belonged to.
Describe how the incident was discovered

The employee called MRD on Oct. 21/11 and spoke with the admin officer there. He explained that he had a printout of the rightful owner's car, make, cylinders, litre capacity and other vehicle details. This prompted the admin officer at MRD to report a confidentiality breach to her manager. An audit was run and 9 of 15 inquiries during that week were not work related. A further audit back to Dec. 2010 revealed 156 inquiries out of 328 that were not work related.

Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised)

80

Type(s) of individuals affected (please check all that apply)

- [ ] Client / Customer / Patient
- [x] Employee
- [ ] Student
- [ ] Other (please specify) some individuals in the general public were accessed but the employee cannot provide a reason.

Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information, replacement of locks, shut down of IT systems, etc.)

Employee was shut out of the MRD system on Oct. 26/11 (immediately following initial audit) and will not regain access until the investigation is completed and any disciplinary measures are decided and implemented.

Personal Information Involved

Describe the personal information involved (e.g. name, address, SIN #, financial information, medical history, etc.) Do not include or send us the identifiable personal information

Either one of two screens were accessed. One screen includes personal info such as birthdate, name, address, weight, height, eye color, medical restrictions as it pertains to driving, fines, points, expiry date. The second screen includes vehicle info such as serial #, licence plate #, driver's licence #, points, model, make, year, insurance company and policy #, cylinders, litres.

Safeguards

Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control

Database information can only be accessed after a user enters a user name and password

Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently at the time of the breach in place to protect the personal information in your custody and control

Database information can only be accessed after a user enters a user name and password

Describe the administration safeguards (policies, procedures, etc.) currently in place to protect the personal information in your custody and control

Employees that have access to personal and private information have received training in how to handle personal and private information.
Describe the administration safeguards (policies, procedures, etc.) in place at the time of the breach to protect the personal information in your custody and control.

Employees that have access to personal and private information have received training in how to handle personal and private information.

Describe the technical safeguards (access controls, audit controls, etc.) currently in place to protect the personal information in your custody and control.

- Encryption
- Password
- Other (please specify)

Describe the technical safeguards (access controls, audit controls, etc.) in place at the time of the breach to protect the personal information in your custody and control.

- Encryption
- Password
- Other (please specify)

Potential Harm

Identify any harm that may result from the breach (please check all that apply)

- Identity theft (higher risk if breach involves SIN # or financial information)
- Physical harm or harassment (e.g. stalking)
- Emotional harm, humiliation or damage to reputation (e.g. disclosure of mental health records)
- Financial cost
- Loss of business or employment opportunities
- Breach of contract and/or other legal obligations (e.g. from data loss)
- Future breaches (technical failures)
- Violation of professional standards or certificate standards
- Risk to public health or safety
- Other (please specify)

Risk

Provide an assessment of the likelihood that harm could result

Consider how likely it is that the subject information can be accessed (e.g. if information was stored electronically, was it encrypted? Was all the information recovered?)
If the information was accessed, consider how likely it is that it can or will be used for fraudulent or otherwise harmful purposes.
Was the information lost or stolen? If stolen, was the information the target of the theft or was it incidental to the theft?
How sensitive is the subject information (e.g. medical information, financial information may be more sensitive).
The risk/likelihood that harm could result is difficult to predict because the individual could not recall or explain a majority of the inquiries. Some were of relatives that he inquired in order to find how old they were on their birthday so he could wish a happy birthday. Others were viewed because he was trying to figure out how a number of traffic fines were falsely sent to him. Still others were an attempt to report income support abusers by accessing them by name or licence plate number. But there was no explanation for many of the inquiries....many are women, some of whom were accessed numerous times. (employees and the general public) Besides accessing the address and birthdate of these individuals, the information might not be classified as overly sensitive. There is a possible chance of identity theft. Due to the multiple times that some of the individuals were accessed and the employee not providing an explanation for these inquiries, there could be possible safety risks for these individuals.

Notification

Has your Senior Privacy Analyst in the ATIPP Office been notified?
☑ Yes Date Analyst was notified: Nov. 16/11
☐ No When will the Analyst be notified

Have law enforcement official been notified?
☐ Yes Who was notified and when?
☑ No Will other authorities be notified at a later time?
☐ Yes If yes, when
☐ No

Have you contacted your solicitor to discuss contractual and/or other legal obligations/impacts?
☑ Yes Who was notified and when? Discussed on Nov. 02/11 at Community of Practice Meeting with Collective Bargaining and met with Dave Martin in Collective Bargaining on Nov. 21/11 regarding appropriate course of action. Initial contact with Department of Justice (ADM Dave Lewis to Todd Stanley) on November 21st - was advised to contact Joe Anthony with any specific questions.
☐ No

Have other authorities (e.g. professional bodies) been contacted?
☐ Yes Who was notified and when?
☑ No Will other authorities be notified at a later time?
☐ Yes If yes, when
☐ No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the primary breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Privacy Breach Report form received by the ATIPP Office

December 1, 2011

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Report form and apply a "Date Received" stamp in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Victoria Woodworth-Lynas

Signature of the ATIPP Office Representative
If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

**Contact Information**

**Department / Public Body:** Government Services

**Division / Program:** Motor Registration Division

**Contact:**

Name: Tom Beckett  
Title: Deputy Registrar  
Phone: 729-2520  
Fax: 729-6955  
E-Mail: beckett@gov.nl.ca  
Mailing address: P.O. Box 8710, St. John's, NL A1B 4J5

**Date of Submission to the ATIPP Office:** December 1, 2011

*(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)*
Risk Evaluation

Incident Description

1. Date the breach occurred: about October 28, 2011
2. Date the breach was discovered: November 23, 2011
3. Describe the breach (provide sufficient detail, including cause):
   The Motor Registration Division mailed a vehicle registration to a customer. Included with this document was a registration renewal and a sticker for a different individual.
4. Location of the breach:
   Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   The vehicle registration and sticker mailed in error has been returned to MRD and couriered to the individual affected. The client affected could not be contacted by telephone. They will be advised by mail and will be offered the opportunity to obtain a new driver licence number and/or a new licence plate for the car. This letter will include an apology for the breach.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, full address, driver's licence number, Vehicle Plate Number, Sticker Number, Document Generation Date, Registration Expiry Date, Make/Model/Style/Colour/Mass/Year/Fuel of the vehicle, Vehicle Serial Number

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   N/A
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to take due care in mailings.

MRD is exploring the option of changing the printing process for vehicle registrations to incorporate the sticker directly into the paper upon which the registration is printed. This will produce a single document which can be processed by the Transportation and Works mailroom for inserting into envelopes by the mailing machine thereby eliminating the manual stapling of stickers to documents and the manual stuffing of envelopes.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - Identity theft (higher risk if breach involves SIN # or financial information)
   - physical harm or harassment (e.g. stalking)
   - emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - financial cost
   - loss of business or employment opportunities
   - breach of contract and/or other legal obligations (e.g. from data loss)
   - future breaches (technical failures)
   - violation of professional standards or certificate standards
   - risk to public health or safety
   - Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - Yes Date Analyst was notified: December 1, 2011
   - No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - Yes Who was notified and when?
   - No Will law enforcement be notified at a later time?
     - Yes
     - No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - Yes Who was notified and when?
   - No

16. Have other authorities (E.g. professional bodies) been contacted?
   - Yes Who was notified and when?
   - No Will other authorities be notified at a later time?
     - Yes
     - No

Important!
You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________
Signature of ATIPP Office Representative
If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: College of the North Atlantic - Qatar

Division / Program: CNA-Qatar

Contact:

Name: Mike Campbell
Title: Project Manager
Phone: 7096437849
Fax:
E-Mail: mike.campbell@cna.nl.ca
Mailing address:

Date of Submission to the ATIPP Office: December 8th 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: unknown
2. Date the breach was discovered: December 2\textsuperscript{nd} 2011
3. Describe the breach (provide sufficient detail, including cause):
   The Project Manager for CNA-Qatar received an anonymous email that contained the following attachments:
   
   Item 1: Internal Memo to former VP - Qatar project. Topic: [blacked out]
   Date of Memo is 29th of April, 2007.
   
   Item 2: Notes of interviews conducted by former CNA-Qatar management. Present in the interviews were [blacked out]. Dated April 11, 2007. Documents contain the names of all persons involved and interviewed.
   
   Item 3. A draft letter [blacked out].

4. Location of the breach: Computer Network / Email Archive CNA-Qatar

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): Item 1 and 2 is 6 people, item 3 is one person

6. Type(s) of individuals affected (check all that apply):
   
   - [ ] Client / Customer / Patient
   - [x] Employee
   - [ ] Student
   - [ ] Other (please specify): Employees' family members

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   
   Viewing of the items listed above has been restricted to CNA executive and senior management involved in the Privacy Breach process.
   
   The College was unsuccessful in its attempt to trace the anonymous email to its source.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:

   Employee Names, Names of parents, names of minor children.

   [blacked out]
Safeguards

9. Describe the **physical** safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   - Network Firewalls, Password protected network access, Logging of activity (including electronic audit trails), Security Cameras, Access Control systems, 24 hour on site security.

10. Describe the **administrative** safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:

    - Information Technology Policy and Procedure monitoring
    - 24 hour on site security
    - Monitoring of associated Human Resource Policy

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

    - [ ] Encryption
    - [x] Password
    - [ ] Other (please specify): access control, Security Cameras
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

☐ Identity theft (higher risk if breach involves SIN # or financial information)
☒ physical harm or harassment (e.g. stalking)
☒ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
☐ financial cost
☐ loss of business or employment opportunities
☐ breach of contract and/or other legal obligations (e.g. from data loss)
☒ future breaches (technical failures)
☐ violation of professional standards or certificate standards
☐ risk to public health or safety
☐ Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

☐ Yes Date Analyst was notified:
☒ No When will the Analyst be notified? 8.12.2011

14. Have law enforcement officials been notified?

☐ Yes Who was notified and when?
☒ No Will law enforcement be notified at a later time?

☒ Yes
☐ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?

☒ Yes Who was notified and when? CNA's General Counsel - December 2, 2011
☐ No

16. Have other authorities (E.g. professional bodies) been contacted?

☐ Yes Who was notified and when?
☒ No Will other authorities be notified at a later time?

☒ Yes
☐ No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

________________________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Service NL

Division / Program: Motor Registration Division

Contact:

Name: Debby Power
Title: Manager of Business Practices
Phone: 709-729-4953
Fax: 709-729-6955
E-Mail: DAPower@gov.nl.ca
Mailing address: PO Box 8710 St John's NL A1B 4J5

Date of Submission to the ATIPP Office: December 19, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: December 13, 2011
2. Date the breach was discovered: December 13, 2011
3. Describe the breach (provide sufficient detail, including cause):

   A copy of a vehicle registration – Town of Winterton as the registered owner was faxed to an incorrect fax number. The same day it was discovered that the fax was received at the Royal Bank in Hearts Content.

4. Location of the breach:
   MRD - Mount Pearl

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): Town of Winterton, Winterton, Trinity Bay.

6. Type(s) of individuals affected (check all that apply):
   ☑ Client / Customer / Patient
   ☐ Employee
   ☐ Student
   ☐ Other (please specify):

7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):

   The Royal Bank in Hearts Content were contacted and an employee reported that this fax was received and shredded when it was discovered the information was not for the bank.

   I contacted Stephanie at the Town of Winterton regarding this error, while she appreciated the call, she had no privacy concerns as the Town is a client of the Royal Bank in Hearts Content and the bank is the holder of all of the Town’s personal information for financial matters.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:

   Registered owner name, address, vehicle plate # and serial # and all vehicle descriptors.

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

   The building is secured with alarms, all doors to areas that contain personal information are have card security. All computers are password protected.
10. Describe the **administrative** safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:

    All staff have received ATIPP training, both online & in person at MRD Mt Pearl. Staff have been directed to cross check fax numbers before the fax is sent. A fax machine security tip sheet is posted next to fax machines.

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

    - Encryption
    - Password
    - Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [ ] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify): This is a low risk breach as the information was received by the clients bank and there were no personal indicators on the document.

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes  Date Analyst was notified: December 16, 2011
   - [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will law enforcement be notified at a later time?
   - [ ] Yes
   - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes  Who was notified and when?
   - [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will other authorities be notified at a later time?
   - [ ] Yes
   - [x] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

__________________________
Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Service NL

Division / Program: Motor Registration Division

Contact:

Name: Debby Power
Title: Manager of Business Practices
Phone: 709-729-4953
Fax: 709-729-6955
E-Mail: DAPower@gov.nl.ca
Mailing address: PO Box 8710 St John's NL A1B 4J5

Date of Submission to the ATIPP Office: December 22, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: December 21, 2011
2. Date the breach was discovered: December 21, 2011
3. Describe the breach (provide sufficient detail, including cause):
   A copy of an accident summary was faxed to an incorrect fax number. This information was requested by the lawfirm Gittens & Associates but was faxed to the lawfirm Inder and Griffen in error.
4. Location of the breach:
   MRD Driver Records Section - Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): Name & address of 2 parties involved in an accident was on the accident summary.
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g., retrieval of breached information; replacement of locks; shut down of IT systems, etc...):
   The staff realized she had faxed it to the wrong number and called the lawfirm Inder & Griffen right away. She spoke to a female who answered the phone and the lady assured her that she would shred the document immediately. Staff never got the name of the individual she spoke to at the law firm.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, address of parties involved in the accident. Vehicle information and estimated damage- dollar value to the vehicles.

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   The building is secured with alarms, all doors to areas that contain personal information are have card security. All computers are password protected.
10. Describe the administrative safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:
All staff have received ATIPP training, online or in person at MRD Mt Pearl. Staff have been directed to cross check fax numbers before the fax is sent. A fax machine security tip sheet is posted next to fax machines.

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [x] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [ ] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify): This is a low risk breach as the information was received by another law firm and document shredded immediately.

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes Date Analyst was notified: December 22, 2011
   - [ ] No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes Who was notified and when?
   - [x] No Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes Who was notified and when?
   - [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes Who was notified and when?
   - [x] No Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: Service NL

Division / Program: Motor Registration Division, Mount Pearl

Contact:

Name: Debby Power
Title: Manager of Business Practices
Phone: 729-4953
Fax: 729-6955
E-Mail: DAPower@gov.nl.ca
Mailing address: PO Box 8710, St John's NL A1B 4J5

Date of Submission to the ATIPP Office: December 29, 2011

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: December 9, 2011
2. Date the breach was discovered: December 29, 2011
3. Describe the breach (provide sufficient detail, including cause):
   A drivers licence belonging to a customer was mailed in error to another customer. The drivers licence was returned to Motor Registration Division on December 29, 2011. I tried to contact the customer to report the breach by telephone but was unsuccessful. A letter was mailed on December 29 offering apologies to what has happened and also giving the customer the option of obtaining a new drivers licence number.
4. Location of the breach:
   Motor Registration Division, Mount Pearl
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 1
6. Type(s) of individuals affected (check all that apply):
   ☑ Client / Customer / Patient
   □ Employee
   □ Student
   □ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   Drivers licence has been returned to Motor Registration Division and staff have been reminded to double check documents before mailing.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, address, drivers licence number.

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   Secure system with password protection.
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
    All staff have received ATIPP training, both online or in person at MRD Mt Pearl. Staff have been ask to cross check documents before mailing to ensure the correct information is going to the correct client.
11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- Encryption
- Password
- Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [x] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] physical harm or harassment (e.g. stalking)
   - [ ] emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - [ ] financial cost
   - [ ] loss of business or employment opportunities
   - [ ] breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] future breaches (technical failures)
   - [ ] violation of professional standards or certificate standards
   - [ ] risk to public health or safety
   - [ ] Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes  Date Analyst was notified: December 29, 2011
   - [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [ ] Yes  Who was notified and when?
   - [x] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will other authorities be notified at a later time?
     - [ ] Yes
     - [x] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

____________________________
Signature of ATIPP Office Representative
If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body: AES

Division / Program: Regional Services

Contact:

Name: Lori Rose
Title: Regional Manager
Phone: 729-7883
Fax: 729-3018
E-Mail: lorirose@gov.nl.ca
Mailing address: 261 Kenmount Road
P.O. Box 8700
St. John’s, NL
A1B 4J6
Risk Evaluation

Incident Description

1. Date the breach occurred: 2011-12-29
2. Date the breach was discovered: 2011-12-29
3. Describe the breach (provide sufficient detail, including cause):
   Service Authorization was issued and sent to the wrong vendor. The authorization for medical transportation was sent to CBS Décor instead of CBS taxi.
4. Location of the breach:
   Conception Bay South, NL
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): 1
6. Type(s) of individuals affected (check all that apply):
   - Client / Customer / Patient
   - Employee
   - Student
   - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   A worker was immediately dispatched to retrieve the document. Document was retrieved, and apologies issued to the vendor. Several attempts were made to reach the client to discuss the breach, but we were unable to reach her by telephone.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Client's name, address and AES case number were on the document

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   n/a
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
Manager has spoken with the Client Services Officer who made the error and reiterated the importance of exercising caution when selecting the vendor from the CAPS system. Matter was also discussed with administrative personnel who print the verified documents and mail them out, so they too will double check the documents before sending. Manager of the Pay Authorization Unit was also alerted

11. Describe the **technical** safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [ ] Encryption
- [ ] Password
- [ ] Other (please specify): N/A
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - [ ] Identity theft (higher risk if breach involves SIN # or financial information)
   - [ ] Physical harm or harassment (e.g. stalking)
   - [ ] Emotional harm, humiliation or damage to reputation (e.g. disclosure of mental health records)
   - [ ] Financial cost
   - [ ] Loss of business or employment opportunities
   - [ ] Breach of contract and/or other legal obligations (e.g. from data loss)
   - [ ] Future breaches (technical failures)
   - [ ] Violation of professional standards or certificate standards
   - [ ] Risk to public health or safety
   - [x] Other (please specify): embarrassment - no risks to client

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - [x] Yes  Date Analyst was notified: 2011-12-29
   - [ ] No  When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will law enforcement be notified at a later time?
     - [ ] Yes
     - [x] No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - [x] Yes  Who was notified and when?
   - [ ] No

16. Have other authorities (E.g. professional bodies) been contacted?
   - [ ] Yes  Who was notified and when?
   - [x] No  Will other authorities be notified at a later time?
     - [x] Yes
     - [ ] No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

IMPORTANT! Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.

Received by:

Signature of ATIPP Office Representative
Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body:  Service NL

Division / Program:  Motor Registration Division

Contact:

Name:  Tom Beckett
Title:  Deputy Registrar
Phone:  729-2520
Fax:  729-6955
E-Mail:  beckettt@gov.nl.ca
Mailing address:  P.O. Box 8710, St. John's, NL A1B 4J5

Date of Submission to the ATIPP Office:  February 1, 2012

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)
Risk Evaluation

Incident Description

1. Date the breach occurred: January 6, 2012
2. Date the breach was discovered: January 19, 2012 - January 31, 2012
3. Describe the breach (provide sufficient detail, including cause):
   The Motor Registration Division generated a new driver licence with a one year renewal as a photo was not available. The licence was to be sent to a person living in British Columbia on a temporary basis. A driver licence for a different person was sent.
4. Location of the breach:
   Clarenville
5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised): One
6. Type(s) of individuals affected (check all that apply):
   ☑ Client / Customer / Patient
   ☐ Employee
   ☐ Student
   ☐ Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc…):
   The individual who received the driver licence in error returned the licence to MRD. As no telephone number was available, the individual whose personal information was exposed was written a letter of apology advising of the privacy breach. We also offered to generate a new driver licence number. The one year renewal driver licence has now been mailed to the correct person.

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). Do not include or send us the identifiable personal information:
   Name, driver's licence number, photo, driver class, date of birth, gender, eye colour, height, date of first licence, signature

Safeguards

9. Describe the physical safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:
   N/A
10. Describe the administrative safeguards (policies, procedures, etc…) currently in place to protect the personal information in your custody and control:
All staff received ATIPP training, not only through the online, but as in-person training sessions with a representative from the ATIPP office. Staff have been directed to cross check information given out. The staff member who mailed the incorrect licence has been spoken to.

11. Describe the technical safeguards (access controls, audit controls, etc…) currently in place to protect the personal information in your custody and control:

- [x] Encryption
- [x] Password
- [ ] Other (please specify):
Potential Harm

12. Identify any harm that may result from the breach (check all that apply):
   - ☑ Identity theft (higher risk if breach involves SIN # or financial information)
   - ☐ physical harm or harassment (e.g. stalking)
   - ☐ emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
   - ☐ financial cost
   - ☐ loss of business or employment opportunities
   - ☐ breach of contract and/or other legal obligations (e.g. from data loss)
   - ☐ future breaches (technical failures)
   - ☐ violation of professional standards or certificate standards
   - ☐ risk to public health or safety
   - ☐ Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?
   - ☑ Yes Date Analyst was notified: February 1, 2012
   - ☐ No When will the Analyst be notified?

14. Have law enforcement officials been notified?
   - ☐ Yes Who was notified and when?
   - ☑ No Will law enforcement be notified at a later time?
     - ☑ Yes
     - ☑ No

15. Have you contacted your solicitor to discuss contractual and/or other legal obligations?
   - ☑ Yes Who was notified and when?
   - ☐ No

16. Have other authorities (E.g. professional bodies) been contacted?
   - ☐ Yes Who was notified and when?
   - ☑ No Will other authorities be notified at a later time?
     - ☑ Yes
     - ☑ No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the Notification Assessment Tool that is available from the ATIPP Office website:

http://www.justice.gov.nl.ca/just/civil/atipp/
For Internal Use by the ATIPP Office Only

Date Reporting form received by the ATIPP Office:

**IMPORTANT!** Upon receipt by the ATIPP Office, please print a copy of the Privacy Breach Reporting form and apply a “Date Received” stamp, in the space provided below. The form must then be immediately forwarded to the Director for review.


**Received by:**

______________________________
Signature of ATIPP Office Representative