



Health and Community Services

Personal Health Information Act
Privacy Audit for the [Organization
Name] [Project Name]

Version

[]

Date:

[date]

TABLE OF CONTENTS

Purposes of This Template	iv
What is a PHIA Privacy Audit?	iv
Concepts	v
Methodology	vii
Organization of the Privacy Audit	xi
Preparation Tips	xiii
Executive Summary	1
1 Introduction	1
1.1 Background	2
1.2 Purpose	2
1.3 Scope and Assumptions	2
1.3.1 Scope	2
1.3.2 Assumptions	3
1.4 Target Risk	3
1.5 Methodology	4
1.6 Information Gathering and Key Personnel	5
2 Privacy Safeguards Verification	6
2.1 Privacy Requirements	6
2.2 Privacy Safeguards	6
2.3 Safeguards Verification Process	6
2.4 Results	7
2.5 Amended Action Plan	9
2.5.1 Deficiencies	9
2.5.2 Action Plan	10
3 Privacy Safeguards Assessment	12
3.1 Assessment Methodology	12
3.1.1 Accountability and Policy	13
3.1.2 Business Processes	13
3.1.3 Technology	13
3.2 Assessment Results	14
4 Privacy Safeguards Confirmation Statement / Privacy Safeguards Deficiencies	16
5 Privacy Endorsement Statement / Action Plan	18
Annex A: References	
Annex B: Privacy Safeguards Effectiveness	

The Personal Health Information Act Privacy Audit Template

PURPOSES OF THIS TEMPLATE

The *Personal Health Information Act* (PHIA) Privacy Audit Template will assist custodians in auditing privacy safeguards following the completion of a PHIA Privacy Impact Assessment (PIA). This template is part of PHIA Risk Management Toolkit prepared by the Department of Health and Community Services, Government of Newfoundland and Labrador.

WHAT IS A PHIA PRIVACY AUDIT?

An audit assesses the effectiveness of controls. In the context of PHIA, the controls are privacy safeguards for personal health information. Audits are an integral part of risk management as the audit process assesses the implementation of privacy safeguards and their effectiveness in addressing risk. The scope of an audit may be limited to one system or project or may include all personal health information in an organization.

Audits can be conducted by internal or external resources and are directed to executive level management and boards of directors. The custodian may have an organizational privacy authority to conduct internal audits. Larger organizations may already have an auditor. Custodians can use reputable auditors for externally-conducted audits occasionally as part of due diligence. This guide is directed towards the conduct of audits by internal resources.

Please see the warning and disclaimer in the introduction to the PHIA Risk Management Toolkit.

When Should a Custodian Conduct a PHIA Privacy Audit?

A custodian should conduct a privacy audit after the completion of a PHIA PIA and its action plan. A template for a PHIA PIA can be found in PHIA Risk Management Toolkit. The custodian should conduct audits regularly, e.g., annually. Custodians may also conduct a privacy audit:

- When a PIA is updated;
- To document that recommended privacy safeguards are implemented;
- To confirm the effectiveness of all privacy safeguards; or
- To assess, on a regular basis, the effectiveness of privacy safeguards to reduce risk to a target acceptable risk level.

Ideally, a privacy audit addresses all safeguards, including security safeguards directed at the confidentiality, integrity and availability of personal health information. Custodians can undertake a privacy audit in parallel with security safeguards testing.


How does a Custodian Benefit from a PHIA Privacy Audit?

PHIA requires custodians to take all reasonable steps to safeguard personal health information. Privacy audits provide an opportunity for custodians to demonstrate due diligence by confirming the effectiveness of privacy safeguards.

In addition, a custodian can use a privacy audit to communicate with provincial and public health authorities regarding the risk management activities it has undertaken. A custodian can also use the privacy audit (or the executive summary of the audit) to communicate with the public or with persons receiving health care regarding how the custodian safeguards personal health information.

Finally, a privacy audit is an opportunity to emphasize the custodian's priorities regarding the protection of personal health information to employees and stakeholders.

Organization of PHIA Privacy Audit Template

The PHIA Privacy Audit Template represents one methodology for conducting a privacy audit and includes instructions embedded in text boxes. The custodian can delete instructional comments when the audit is complete. Each set of embedded instructions in the privacy audit template starts with this symbol: 

CONCEPTS

Custodians should understand the concepts used in the privacy audit tool before proceeding with an audit:

Confirmation	A process for documenting and stating the residual risk for operations, a system or a program.
Endorsement	The acceptance by executive management of residual risk, as identified in the confirmation statement.
Safeguards	A privacy safeguard is effective if it reduces risk to the target risk

Effectiveness	level. The effectiveness ratings used in the privacy audit template are Low, Moderate and High.
Risk	<p>The PHIA PIA template explains risk, residual risk and target risk. The basic definitions are repeated for convenience:</p> <p>Risk is a function of likelihood and impact: Likelihood means the probability that an event will occur. The following definitions apply to rating the likelihood of an event:</p> <p>Low: There is little history inside the organization or elsewhere and the threat is considered unlikely to occur.</p> <p>Moderate: There is some history inside the organization or elsewhere and the threat could occur.</p> <p>High: There is significant history inside the organization or elsewhere and the threat is likely to occur.</p> <p>Impact means the magnitude of damage should the event occur. Impact can be on the custodian, on the owner of the personal health information or on both. Impact can include loss of reputation, embarrassment, financial loss, loss of livelihood, or other negative consequences. The magnitude of the impact may be difficult to measure: something that has a low impact on a large custodial organization may be significant to a small organization. Defining impact will help the custodian's employees and third party partners and stakeholders to understand the consequences of failing to apply privacy safeguards and demonstrates to other organizations how the custodian has arrived at conclusions about risk. The following definitions apply to rating the impact of an event:</p> <ul style="list-style-type: none"> • Low: Little or no damage could result if the event occurs. • Moderate: Serious damage could result if the event occurs. • High: Extremely serious damage could result if the event occurs. <p>Once likelihood and impact have been rated, the custodian can arrive at a Risk Rating of Low, Moderate or High.</p> <p>Conducting a PIA or a privacy audit is an opportunity to discuss risk in terms of likelihood and impact and to communicate examples of low, moderate or high impact internally.</p>

Residual Risk	The risk that remains after the implementation of all privacy safeguards. The risk definitions used in PHIA PIA template are repeated here for convenience: <ul style="list-style-type: none">• Low – There is a possibility that a risk will materialize but there are mitigating factors;• Moderate – There is a strong possibility that a risk will materialize if no corrective measures are taken; and• High – There is a near certainty that the risk will materialize if no corrective measures are taken.		
Risk Rating	The risk rating table below shows how likelihood and impact are combined to arrive at risk ratings.		
Risk Rating Table			
Likelihood	Impact		
	Low	Moderate	High
Low	Low	Low to Moderate	Moderate
Moderate	Low to Moderate	Moderate	Moderate to High
High	Moderate	Moderate to High	High

METHODOLOGY

PHIA Privacy Audit assesses the effectiveness of privacy safeguards. This means that the audit verifies that safeguards are in place, that they address requirements in legislation and policy, and that they are effective in reducing risk to the target acceptable level of risk.

A number of approaches are legitimate; this Privacy Audit methodology is based on three building blocks:

1. Verify privacy safeguards against requirements	Includes documenting that all privacy safeguards have been implemented and matching them to requirements.

2. Assess and confirm privacy safeguards' effectiveness	Analogous to the certification process in security safeguards implementation, when technical staff members test security safeguards to confirm that they operate as expected and identify residual risk.
3. Endorse privacy safeguards	Analogous to accreditation in security safeguards implementation, when executive management accepts residual risk.

The paragraphs below describe each of the three building blocks of the privacy audit.

1. Privacy Safeguards Verification

The PHIA PIA template is the starting point for safeguards verification. The aim of privacy safeguards verification is to confirm that the custodian has addressed all risks, i.e. that planned and recommended privacy safeguards are implemented and that collectively, they address all requirements. This process should be repeated if it identifies gaps. The result is a Privacy Safeguards Verification report, which is Section 2 of the privacy audit template. The activities should include the following:

Map planned and recommended privacy safeguards to requirements	<p>Use Annex C, the list of Privacy Safeguards, and the privacy risk assessment in Section 6 of the PHIA PIA to prepare a list of recommendations that are matched to requirements.</p> <p>The second column, which is labeled Privacy Safeguards, in Annex B of this template, acts as a verification checklist: the safeguards listed are what the custodian must verify are in place. The requirements the safeguards address are listed in the first column, which is labeled Requirements.</p>
Verify that each privacy safeguard has been implemented	<p>Use the verification checklist to confirm that the privacy safeguards have been implemented and are used to address the requirements as planned in the PIA.</p> <p>Consult with business and technology managers to ensure accuracy and completeness.</p>

Document results.	Report on findings: Check all implemented privacy safeguards against the requirements they address using the Implementation column in Annex B and the ✓ symbol in the space provided; and note deficiencies if any by placing a ✕ symbol in the space provided.
Revise the action plan as required	Revise Section 8 of the PIA, which is the Action Plan, as required and insert the amendments into Section 2 of this Privacy Audit.

2. Privacy Safeguards Confirmation

This process is not undertaken until the custodian has verified that all privacy safeguards are in place as reported in Section 2 of the privacy audit template. Then the custodian is ready to confirm that privacy safeguards address privacy risks as anticipated, i.e. that they reduce risk to the target risk level. This building block is the Privacy Safeguards Confirmation. It requires preparation and time for testing the effectiveness of safeguards by using a variety of techniques as described below.

Prepare a plan	<ul style="list-style-type: none"> • Use information from the safeguards verification to develop the plan, including identifying priorities. • Plan to address all safeguards. • Incorporate threat and risk assessment information, security confirmation and endorsement reports, training plans, policy and standards, directives and other information that may assist in confirming the effectiveness of privacy safeguards.
Assess privacy safeguards	<ul style="list-style-type: none"> • Use the safeguards verification report, which is Section 2 of this template, and the Action Plan in the PIA to identify managers and the safeguards for which they are accountable. • Assess the effectiveness of all procedures, processes, policy, agreements, technology and other activities that constitute the privacy safeguards. Use the tools

	<p>developed in the preparation phase.</p> <ul style="list-style-type: none"> • Confirm that employees, partners and stakeholders understand and apply required processes, procedures and other privacy safeguards. • Review privacy incidents and complaints, including their resolution and follow-up action. • Interview a select number of personal health information owners, if possible.
Document safeguards' effectiveness	<ul style="list-style-type: none"> • Document the effectiveness of safeguards in the Effectiveness column of Annex B of this template. • Rate privacy safeguards as they apply singly or in concert for each requirement. Use the rating system defined in this guide and in Section 3 of the Privacy Audit Template.
<p>Prepare a confirmation statement</p> <p>OR</p> <p>Prepare a statement of deficiencies</p>	<p>State the residual risk for each privacy principle and as well as residual risk for the system or organization.</p> <p>OR</p> <p>If residual risk remains higher than the target risk, prepare a list of deficiencies.</p>

3. Safeguards Endorsement

The custodian's executive management normally accepts the results of safeguards confirmation if the overall residual risk is at the target acceptable level. Acceptance of the confirmation statement is formal acceptance of the residual risk identified in the confirmation statement and constitutes endorsement.

If there is a statement of deficiencies, prepare an action plan:

- Recommend strengthened or replacement privacy safeguards that will reduce risk.
- Incorporate recommendations in a prioritized action plan, which is the response to the report of deficiencies. The action plan tables in Section 8 of the PIA can be used to set out the action plan.
- In this case, the audit team obtains approval from executive management and corrects deficiencies as set out in the prioritized action plan.

- Once the action plan is completed, the audit team should confirm safeguards effectiveness and obtain executive management's endorsement.

ORGANIZATION OF THE PRIVACY AUDIT

The audit is organized into the following sections, each of which is described in more detail within the template itself. The custodian can provide additional information in annexes as suggested in the table below.

Section 1: Introduction	<p>The Introduction summarizes the background for the project, system or organization; the purpose, scope and assumptions; the target risk; methodology; and resources. Annex A lists resources consulted.</p>
Section 2: Privacy Safeguards Verification	<p>This section contains a summary of the privacy safeguards that are intended to reduce risk to the target acceptable level. Annex B is a detailed privacy safeguards checklist mapped to each privacy requirement as set out in the PIA report.</p>
Section 3: Privacy Safeguards Assessment	<p>This section describes how each safeguard has been assessed for its effectiveness, i.e. the tests, inspections or other activities the auditor used. Annex B includes the documentation, processes, and technology that support each privacy safeguard as well as a rating of the effectiveness of each safeguard or group of safeguards when they act as a group.</p>
Section 4: Privacy Safeguards Confirmation Statement OR Privacy Safeguards Deficiencies	<p>The Privacy Safeguards Confirmation Statement section confirms that the residual risk is the same as the target risk.</p> <p>OR</p> <p>If the residual risk is higher than the target risk, this section is called Privacy Safeguards Deficiencies that identifies risk levels that are higher than the target risk level.</p>

<p>Section 5: Privacy Safeguards Endorsement Statement</p> <p>OR</p> <p>Action Plan</p>	<p>The Privacy Safeguards Endorsement statement accepts residual risk if the residual risk is certified as being the same as the target risk.</p> <p>OR</p> <p>If there were deficiencies, this section is the Privacy Safeguards Implementation Action Plan and constitutes the response for correcting deficiencies identified in Section 4.</p>
---	--

PREPARATION TIPS

Custodians that have decided to audit privacy safeguards for a system, business line or for the organization can consider the following steps to prepare for the audit:

Assemble an audit team: Even if an outside resource conducts the audit, the auditor will need to consult internal resources to ensure that information is complete and accurate. It is important that the audit be conducted openly and in as collaborative a manner as possible. The audit team needs to consult stakeholders and participants in an initiative or project, including planners, business managers, records managers, information technology experts, and partners and third party service providers. To keep the consultation process manageable, only accountable individuals should participate; others can be consulted as required.

Assemble reference materials: Examine documents that outline business plans, requirements, concept of operation, technology, threat and risk, processes, Accountability, partnerships, information models and any other material that will help assess risk to personal health information. The following are available as part of the PIA toolkit:

- Completed Preliminary Privacy Impact Assessment questionnaire, if used;
- Completed PHIA PIA; and
- *PHIA Policy Development Manual*.

Ensure that a completed PHIA PIA template is available. The PHIA PIA template is the starting point for the audit; the audit team will use information in the PIA throughout the audit. Obtain copies of incident reports and identify trends; examine follow-on activities. Identify changes or additions to privacy safeguards if any.

Prepare an audit plan: An audit plan with deliverables and milestones is useful for measuring progress and reporting. The plan will determine the scope and objectives of the audit. Post the plan on an internal web site if possible or distribute it widely.

Identify and develop assessment methodology and tools: The variety in types of privacy safeguards will require a variety of tools for measuring their effectiveness. For some, effectiveness will be difficult to quantify. Ensure that this activity includes identifying who to interview or provide with a questionnaire or survey. Questionnaires, surveys, interviews and other methods can be used to measure safeguards' effectiveness. The custodian's web site may be one way to gather information from external sources. Privacy incident reporting is one way to decide which safeguards to examine with the greatest rigour.

Brief executives: Ensure that organizational executives understand the audit and potential outcomes.

Identify budget: Identify resources and limitations for implementing recommendations. If risk has not been reduced to the target risk, an action plan to address risk is required. Identifying resource limitations will help the auditor to develop a realistic action plan.

Executive Summary



*The **Executive Summary** is intended for non-program and non-technical audiences. It should briefly describe what has been verified and tested; and the results. It reports its conclusions regarding privacy safeguards effectiveness, identifies how and when deficiencies, if any, will be corrected.*

The Executive Summary is written when the privacy audit is complete.

This privacy audit assesses privacy safeguards for personal health information by using the Government of Newfoundland and Labrador Privacy Audit methodology to examine the effectiveness of health information protection practices and risk management for [Organization Name] [Project Name].

The privacy analysis concludes that... <Insert Conclusions>:



Insert the conclusions of the audit, including a list of deficiencies if any, and identify when deficiencies will be corrected.

The amended action plan will be completed by <Insert Date>.



*An **audit** assesses the effectiveness of controls: in this case, the controls are privacy safeguards. Audits are integral to risk management. PHIA Privacy Audit verifies the implementation of privacy safeguards and their effectiveness in addressing risk to personal health information. The scope of a privacy audit may be limited to one system or project or may include all personal health information in an organization.*

A privacy audit follows completion of a PHIA PIA and implementation of recommended safeguards.

Custodians should use this template as a guide, and tailor content and organization to suit their requirements.

Custodians should delete embedded text when the audit is complete.

1 INTRODUCTION



*The **Introduction** sets the stage by briefly describing the organizational operations, system or program and the privacy audit's purpose and scope. Information in the introduction helps internal and external stakeholders to understand what the privacy audit applies to and helps to focus the privacy audit team. The introduction can state assumptions, describe the methodology, identify resources, and define the terms used in the privacy audit.*

The sections below include sample text and additional explanations.

This document describes the privacy audit conducted for the [Organization Name] [Project Name].

1.1 BACKGROUND

The business purpose of [Project Name] is to...<Insert Background Information>.

1.2 PURPOSE



*The **Purpose** describes what the privacy audit is for. Custodians use privacy audits to measure the effectiveness of privacy safeguards over time. Audits can be internal or external and are directed to executive level management.*

The purpose of the privacy audit is to provide senior management with information that supports informed risk management decisions relating to personal health information in the [Project Name] system.

1.3 SCOPE AND ASSUMPTIONS



***Scope and Assumptions section** describes what is included in the privacy audit, what is excluded from the privacy audit and the assumptions that govern the privacy audit.*

1.3.1 SCOPE



*The **Scope** should define what is being audited and the level of detail. Executive management may also define the scope of an audit. It is important to define what is included and what is excluded from the audit so that stakeholders and partners understand the audit's conclusions and recommendations.*

The focus of the privacy audit is the personal information of <patients, etc> that will reside in [Project Name]. It is an internal audit that describes the following:

- a. The privacy safeguards for [Organization Name] [Project Name] as described in the PHIA PIA; and
- b. [Etc.]

1.3.2 ASSUMPTIONS



*The custodian can list all **Assumptions**: assumptions are anything that could affect the audit, e.g. completeness of information available, validity of test results, etc. The custodian can clarify factors affecting the audit, such as anticipated performance of a technology, hiring of adequate resources, completeness of information, or accuracy of information.*

The privacy audit is based on...<Insert where assumptions came from (e.g. interviews, documentation, etc)>. The following assumptions have been made:
<Insert assumptions>

- a. ;
- b. ; and
- c.

1.4 TARGET RISK



*The custodian assesses privacy safeguards for their effectiveness in reducing risk to the **target risk**, which is normally Low, as identified and defined in the PHIA PIA and in the text below. The custodian's executive management can identify target risk.*

The <Insert Title of the PHIA PIA>. identifies the target privacy risk as <Insert Target Risk>.

The <Insert Title of the PHIA PIA>. quantifies risk as follows:

Low – There is a possibility that a risk will materialize but there are mitigating factors;

Moderate – There is a strong possibility that a risk will materialize if no corrective measures are taken; and

High – There is a near certainty that the risk will materialize if no corrective measures are taken.

1.5 METHODOLOGY



The Methodology used in this template consists of three building blocks, each of which builds on its predecessor. A PHIA PIA is the starting point for the audit.

The first step is to verify that privacy safeguards listed in the PHIA PIA are in place and then identify the requirements that each addresses. At the end of this step, the custodian will have accounted for all privacy safeguards. Section 2 describes this step in more detail. The safeguards and requirements are listed in Annex B.

The second step is to assess and confirm that the privacy safeguards reduce risk to the target level of risk or to identify deficiencies. Section 3 describes this step in more detail. The third step is to endorse the organization's operations, system or program by accepting residual risk or to establish an action plan for reducing risk to the target risk. Section 4 describes this step in more detail.

Information in this privacy audit is organized into the following sections:



The privacy audit template is organized to follow the audit methodology, and consists of the five sections listed:

***Section 1: The Introduction** summarizes the background for the project, system or organization; the purpose, scope and assumptions; the target risk; methodology; and resources. Annex A lists resources consulted.*

***Section 2: Privacy Safeguards Verification** contains a summary of the privacy safeguards that are intended to reduce risk to the target risk. Annex B is a detailed privacy safeguards checklist mapped to each privacy requirement as set out in the PIA.*

***Section 3: The Privacy Safeguards Assessment** describes how each safeguard has been assessed for its effectiveness. Annex B includes the documentation, processes, and*

technology that support each privacy safeguard as well as a rating of the effectiveness of each safeguard or group of safeguards when they act as a group.

Section 4: The Privacy Safeguards Confirmation Statement confirms that the residual risk is the same as the target risk. If the residual risk is higher than the target risk, this section is called *Privacy Safeguards Deficiencies* and it identifies risk levels that are higher than the target risk level.

Section 5: The Privacy Safeguards Endorsement accepts residual risk. Normally this means that the residual risk has been confirmed as being the same as the target risk. If there were deficiencies, this section is the *Privacy Safeguards Implementation Action Plan* and constitutes the response for correcting deficiencies identified in Section 4.

The Privacy Safeguards Endorsement is not completed until residual risk is the same level as the target risk.


1.6 INFORMATION GATHERING AND KEY PERSONNEL



The custodian can summarize the resources that contributed to the audit through interviews, group sessions and documentation; and can list detailed information about resources and documents in Annex A.

Annex A lists documents and individuals consulted in the preparation of this privacy audit.

2 PRIVACY SAFEGUARDS VERIFICATION

 The **Privacy Safeguards Verification** is the first step in the privacy audit. This section describes the privacy safeguards and the requirement(s) that each addresses. It reports on which privacy safeguards are in place and which are not, if any. It identifies deficiencies and gaps, if any. It should summarize the privacy checklist in Annex B, which is a detailed list of privacy safeguards and of legislated and policy requirements.

When this section is complete, the custodian will have verified the status of each privacy safeguard and recorded that status in Annex B. The custodian can then use the verification to amend the PHIA PIA action plan, if necessary.


Annex B is a privacy safeguards checklist.

2.1 PRIVACY REQUIREMENTS

 The custodian can list the **Privacy Requirements** from Annex C of the PHIA PIA in the Requirements column in Annex B of this privacy audit template, and summarize them below.

The privacy requirements are listed in the first column of the tables in Annex B.

2.2 PRIVACY SAFEGUARDS

 The custodian can use Annex C to the PHIA PIA to enter the **Privacy Safeguards** in the second column of Annex B to this privacy audit template, and summarize the privacy safeguards below.

The second column of Annex B lists all privacy safeguards; Annex C to the PHIA PIA describes each safeguard in detail. The action plan to implement privacy safeguards implementation was completed on XYZ date.

2.3 SAFEGUARDS VERIFICATION PROCESS



*The **Safeguards Verification Process** describes how the custodian verified that privacy safeguards are in place. The custodian uses the Implementation column of Annex B to record detailed information about safeguards verification and summarizes the processes below.*

The custodian can organize this section into the ten privacy principles and combine it with Section 2.4 Results. If preferred, the custodian can organize according to the type of privacy safeguard, e.g. policy and Accountability, security, training and awareness etc. Verification can include interviews, questionnaires, physical inspections and any other record associated with privacy safeguards.

NOTE: The verification process simply verifies that safeguards exist. It does not assess their effectiveness.



2.4 RESULTS



*The custodian summarizes the **Results** of the verification by identifying privacy safeguards that have been fully implemented and deficiencies and gaps if any; the Implementation column of Annex B provides detailed information about verification results. The results can be organized to reflect the organization of Annex B, i.e. according to the ten privacy principles.*

If the custodian identifies deficiencies in privacy safeguards implementation, the custodian will need to amend the Action Plan from Section 7 of the PIA. Deficiencies or gaps may be privacy safeguards that have not been implemented at all, safeguards that are in the course of being implemented, or safeguards that were implemented but are no longer being used.

Table 1: Safeguards Verification Results

Privacy Principle	Implementation (Y/N)	Deficiencies
Accountability	 The custodian indicates Yes if all privacy safeguards for this privacy principle are in place and No if there are gaps.	 The custodian lists any deficiencies or gaps in privacy safeguards. There can be more than one for each privacy principle.
Identifying Purposes		
Consent		
Limiting Collection		
Limiting Use, Disclosure and Retention		
Accuracy		
Safeguards		
Openness		

Individual Access		
Challenging Compliance		




2.5 AMENDED ACTION PLAN

 *The custodian prepares an **Amended Action Plan** to address deficiencies.*

2.5.1 DEFICIENCIES

The verification identifies the following deficiencies, as listed in Annex B with the privacy principle and requirement that each should address. Deficiencies will be listed in Table 2, below.

Table 2: Safeguards Deficiencies

Privacy Principle	Requirement	Deficiency
 <i>Insert the privacy principle that the deficiency applies to. There may be more than one deficiency for each principle or none.</i>	 <i>Insert the requirement for which there are no privacy safeguards in place.</i>	 <i>List the safeguard(s) that were intended to address the requirement and how they are deficient, e.g. Being implemented but not complete; Not implemented.</i>
Accountability	Appoint a custodian	Custodian not yet appointed

2.5.2 ACTION PLAN

The Health PIA Action Plan in Section 7 of the Health PIA has been amended to address deficiencies identified above. The amendments listed below:

No: <Sequential #>		Requirement Addressed: < Insert Privacy Principle and specific requirement>			Privacy Safeguards Category: <Insert Category, e.g. Management, Business, Operations, Technical, Security>	
Activity Name: <Name of Activity that will implement specific recommendations from Section 6>						
Activity Description: <Description of the activity that will implement specific recommendations from Section 6>						
Resource Requirements: <Insert estimated total of days effort and/or estimated total cost for completing this activity>						
Resource / Individual	Recommendation Number	Recommendation Title	Costs and / or allocations Required	Target Date	Accept (Yes/No)	Organization Decision

No: <Sequential #>		Requirement Addressed: < Insert Privacy Principle and specific requirement>			Privacy Safeguards Category: <Insert Category, e.g. Management, Business, Operations, Technical, Security>	
Activity Name: <Name of Activity that will implement specific recommendations from Section 6>						
Activity Description: <Description of the activity that will implement specific recommendations from Section 6>						
Resource Requirements: <Insert estimated total of days effort and/or estimated total cost for completing this activity>						

Resource / Individual	Recommendation Number	Recommendation Title	Costs and / or allocations Required	Target Date	Accept (Yes/No)	Organization Decision

3 PRIVACY SAFEGUARDS ASSESSMENT



*Now that the custodian has documented the implementation of each safeguard, the custodian conducts the **Privacy Safeguards Assessment**. This section summarizes how the custodian measured the effectiveness of each privacy safeguard or combination of privacy safeguards. It refers to detailed information in Annex B. This is the second step in the privacy audit.*

Annex B lists each safeguard and how it is implemented in policy, processes or technology, and assigns an effectiveness rating for each safeguard or group of safeguards of Low, Moderate or High. The effectiveness rating is based on tests, inspections or other ways of measuring effectiveness.

When this step is completed, the custodian will have documented the privacy assessment including the results.

This section describes how the audit team assessed the effectiveness of all privacy safeguards implemented for the [Project Name]; privacy safeguards that are intended to operate in combination with other safeguards were assessed in combination.

The effectiveness ratings are defined as follows:

- **Low** – The privacy safeguard marginally reduces risk;
- **Moderate** – The privacy safeguard reduces risk measurably but not adequately; and
- **High** – The privacy safeguard reduces risk to the target risk level.

3.1 ASSESSMENT METHODOLOGY




*The **Assessment Methodology** summarizes how the custodian assessed the effectiveness of privacy safeguards. It describes the assessment of each category of privacy safeguard in the order provided in Section 2 and in annexes B and C. The custodian can attach the assessment plan as an annex, if desired, and refer to it in this section.*


The summary should describe each activity used to assess safeguards effectiveness; the activities can include any or all of the following:

- **Interviews with responsible managers:** Use the privacy safeguards verification report and the PHIA PIA Action Plan to identify managers and the safeguards for which they are accountable.
- **Tests** of all procedures, processes, policy, agreements, technology and other activities that constitute the privacy safeguards; test tools can include interviews, surveys, and analysis.
- **Confirmation** that employees, partners and stakeholders understand and apply required processes and procedures.
- **Review** of privacy incidents and complaints, including resolution and follow-up action.
- **Interviews** with selected personal health information owners, if possible.


3.1.1 ACCOUNTABILITY AND POLICY

 **Accountability and Policy** summarize how the custodian assessed the effectiveness of accountability and policy, including the use of surveys, questionnaires, focus group sessions or other methods. Copies of questionnaires or surveys can be attached as appendices to Annex C.

3.1.2 BUSINESS PROCESSES

 **Business Processes** summarize how the custodian assessed the effectiveness of processes or procedures, including the use of process challenges, observation, interviews or questionnaires. Copies of assessment material can be attached as appendices to Annex C.

3.1.3 TECHNOLOGY

 **Technology** summarizes how the effectiveness of technical privacy safeguards was assessed, including tests. Copies of tests can be attached as appendices to Annex C.

3.2 ASSESSMENT RESULTS



 The custodian needs to **document safeguards effectiveness** by recording the rating in the Effectiveness column in Annex B.

The custodian can **summarize** in Section 3.2 how well the privacy safeguards reduce risk. The custodian can organize the summaries according to the categories of privacy safeguards used in Annex C to the PHIA PIA. This method highlights weaknesses and strengths according to categories of privacy safeguards. An alternative is to organize according to the ten privacy principles, which highlights weaknesses and strengths according to requirements for safeguarding personal health information.

The table below organizes the summary into the ten privacy principles.


The table below lists the safeguards effectiveness for each privacy principle and the residual risk for each.

Table 3: Safeguards Effectiveness and Residual Risk

Privacy Principle	Safeguards Effectiveness	Residual Risk
Accountability	 Insert overall safeguards effectiveness rating of Low, Moderate or High.	 Insert overall residual risk rating of Low, Moderate or High.
Identifying Purposes		
Consent		
Limiting Collection		
Limiting Use, Disclosure and		

Retention		
Accuracy		
Safeguards		
Openness		
Individual Access		
Challenging Compliance		

4 PRIVACY SAFEGUARDS CONFIRMATION STATEMENT / PRIVACY SAFEGUARDS DEFICIENCIES

 This section documents the **third step** in the privacy audit. It states the overall level of residual risk and the level of residual risk for each of the ten privacy principles. This section is a summary of detailed information from the **Effectiveness** columns in Annex B.

If privacy safeguards have reduced residual risk to the target risk, this section finishes with a statement that confirms that the safeguards have achieved the target risk.
 If the level of residual risk is higher than the target risk, this section identifies deficiencies in detail and recommends corrective action, such as strengthening existing privacy safeguards or adding new privacy safeguards.

When this step is completed, the custodian will know where risk needs to be addressed.

The residual risk for [Organization Name][Project Name] is rated as <Insert Residual Risk Rating of Low, Medium or High>.




 If the overall residual risk rating is higher than the target risk, provide a list of deficiencies, identify risk and recommend corrective action. The table below is a suggested format.

Table 4: Recommendations for Addressing Risk

Privacy Principle	Deficiency and Risk	Recommended Action
Accountability	 List deficient safeguards if any and describe risk for each i.e. what will happen as a result of deficient.	 Recommend additional or strengthened safeguards to reduce risk to target risk.

Privacy Principle	Deficiency and Risk	Recommended Action
Identifying Purposes		
Consent		
Limiting Collection		
Limiting Use, Disclosure and Retention		
Accuracy		
Safeguards		
Openness		
Individual Access		
Challenging Compliance		

5 PRIVACY ENDORSEMENT STATEMENT / ACTION PLAN



*The **Privacy Endorsement Statement** is executive level management's acceptance of residual risk, which is normally the same as the target risk, as stated in Section 4, the Privacy Confirmation Statement.*

If Section 4 does not confirm that residual risk is the same as target risk, this section contains a prioritized action plan for addressing the deficiencies identified in Section 4. The action plan can use the table formats in Section 8 of the PIA template, which are also used in Section 2.5 of this report.

The custodian can include a chart to depict relationships and dependencies.

The table below lists the persons who contributed directly to this audit.

The table below lists the documents used in preparing this audit.

Version []

Annex B – Privacy Safeguards’ Effectiveness



The custodian can extract the **Privacy Safeguards** from Section 5 of the PIA. The organization of information in this annex parallels the organization in the PHIA PIA template, i.e. it is organized into the ten privacy principles from the CSA Model Code.

A privacy safeguard is effective if it reduces risk to the target risk. The effectiveness ratings used in the privacy audit template are Low, Moderate and High, as defined below:

- **Low** – The privacy safeguard marginally reduces risk;
- **Moderate** – The privacy safeguard reduces risk measurably but not adequately; and
- **High** – The privacy safeguard reduces risk to the target risk level.

This annex supports the privacy safeguards verification in Section 2, the privacy safeguards assessment in Section 3 and the confirmation statement in Section 4.

Privacy safeguards that are rated as **Low** or **Moderate** may be deficient and therefore may not reduce risk to **Low** when applied; privacy safeguards that when applied individually or with other privacy safeguards to achieve a rating of **High** are considered to be effective in reducing risk.

Principle 1 – Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.






The custodian uses the ten tables in Annex B to provide detail for Sections 2 and 3 of the privacy audit.

*The **Requirement column** on the left lists all of the requirements that custodians need to address under PHIA. The custodian can add requirements that were identified in the PHIA PIA. The custodian completes the requirements column for all privacy principles and lists the privacy safeguards that apply to each.*

*To complete the **Privacy Safeguards Verification in Section 2**, the custodian uses each **Implementation column** to describe how the custodian has verified that each safeguard is in place, e.g. by reviewing documentation, using questionnaires, interviewing managers, etc. The custodian notes deficiencies in Section 2 of this Privacy Audit and uses them to amend the PIA Action Plan.*

*To complete the **Privacy Safeguards Assessment in Section 3**, the custodian uses each **Effectiveness column** to rate each safeguard or combination of safeguards, based on tests of privacy safeguards effectiveness. The custodian describes the tests used for the assessment in Section 3 of the privacy audit.*

Requirement	Privacy Safeguards	Implementation	Effectiveness
Designate a person to make a decision required of a custodian under PHIA.	 <i>List each safeguard that applies to the requirement in the Requirement column. This column in combination with the Requirement column, acts as a verification checklist.</i>	 <i>In the column immediately to the right, enter a ✓ if the safeguard is in place or an ✗ if the privacy safeguard is not in place. This column is completed for Section 2, Privacy Safeguards Verification.</i>	 <i>Insert the risk rating following assessment of safeguards effectiveness. This column is completed for Section 3, Privacy Safeguards Assessment.</i>
Designate one or more contact persons to perform the following functions: <ul style="list-style-type: none"> Facilitate the custodian's 			

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>compliance with this Act and the regulations;</p> <ul style="list-style-type: none"> • Ensure that employees, contractors, agents and volunteers of the custodian and those health care professionals who have the right to treat persons at a health care facility operated by the custodian are informed of their duties under this Act and the regulations; • Respond to inquiries from the public in respect of the custodian's information policies and procedures; and 				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<ul style="list-style-type: none"> Respond to requests by an individual for access to or correction of personal health information about the individual that is in the custody or under the control of the custodian. <p>NOTE: When the custodian does not identify a contact person, the custodian, if an individual rather than an organization, is considered to be the contact person. The custodian makes his or her contact information available in accordance with Section 18 of PHIA.</p>				
Establish and implement privacy policy and procedures to facilitate the				

Requirement	Privacy Safeguards	Implementation		Effectiveness
implementation of, and ensure compliance with, PHIA and regulations respecting the manner of collection, storage, transfer, copying, modification, use and disposition of personal health information whether within or outside the province. The policy and procedures should include all elements identified in Part II, Section 13.				
Identify third parties involved in custody or control of the personal information and establish legal arrangements regarding privacy requirements.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
Require employees, agents, contractors, volunteers and, where applicable, health care professionals who may treat patients in the custodian's health care facility, to take an oath or affirmation of confidentiality.				
Ensure that employees, agents, contractors, volunteers and, where applicable, health care professionals who may treat patients in the custodian's health care facility, comply with the provisions of PHIA, any Regulations promulgated under PHIA, and with the custodian's information policies and procedures.				

Principle 2 – Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>On collection of personal health information, take reasonable steps to inform the individual or his or her representative:</p> <ul style="list-style-type: none"> • of the purpose for the collection, use and disclosure of the information; • of the identity of and other relevant information relating to the contact person referred to in Section 18; 				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>and</p> <ul style="list-style-type: none"> of other information prescribed in the regulations as described in Part II, Section 20 of PHIA. 				

Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Requirement	Privacy Safeguards	Implementation		Effectiveness
Obtain consent directly from the individual who is the subject of the information or from their duly appointed authorized representative, except as collection, use and / or disclosure without consent is permitted in Part IV of PHIA.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
Where consent is not obtained from the individual who is the subject of the information or from their duly appointed authorized representative, ensure that the collection, use and / or disclosure without consent is permitted in Part IV of PHIA.				
Consent shall be knowledgeable and not obtained through deception or coercion.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
Obtain express consent when personal health information is to be disclosed outside of the “circle of care”, whether to a non-custodian or to the custodian for purposes other than for health care.				
Inform custodians with whom personal health information is shared of any limitations placed on disclosure by the individual patient.				
Provide for individuals to withdraw consent to collection, use or disclosure.				

Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Requirement	Privacy Safeguards	Implementation		Effectiveness
Limit collection of personal health information to that which is reasonably necessary to meet the purpose of the collection, except where the collection is required by law.				

Principle 5 – Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Requirement	Privacy Safeguards	Implementation		Effectiveness
Limit the use of personal health information to the minimum amount of information necessary to achieve the purpose for which it is being used.				
Limit the disclosure of personal health information to the minimum amount of information necessary to accomplish the purpose for which it is used, unless disclosure is required by law.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
Personal health information is not to be used or disclosed if other information will serve the purpose and only if consent is obtained for its use or disclosure.				
Disclose personal information only with the consent of the individual or where specifically authorized under Part IV.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Use personal health information for the purpose for which the information was collected.</p> <p>NOTE: Section 34 of PHIA sets out permitted uses in detail.</p>				
<p>Limit the use of personal health information to employees or agents who require the information to carry out the purpose for which the information was collected or for a purpose authorized under PHIA.</p>				

Requirement	Privacy Safeguards	Implementation		Effectiveness
When transferring records of personal health information to a successor custodian, take reasonable measures to notify the individual who is the subject of the information prior to the transfer or as soon as possible after the transfer regarding the transfer of information, including identification of the successor custodian.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
Ensure consent is obtained prior to disclosure of personal health information outside the province, and that the disclosure is permitted under PHIA as set out in section 47 of PHIA. The disclosure should only be to a person whose functions are similar to those performed by the disclosing custodian.				
Record all disclosures of personal health information, including name, date and purpose, and description of information disclosed, including the use of automatic logging for electronic health records.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Where the custodian uses or discloses personal health information about an individual without the individual's consent in a manner that is inconsistent with the information policies and procedures referred to in Section 13, the custodian shall:</p> <ul style="list-style-type: none"> ▪ Inform the individual who is the subject of the information of the use or disclosure at the first reasonable opportunity except where, under Section 58, the custodian would be required or permitted to refuse access to the record of personal health information; ▪ Make a note of the use or disclosure; and, 				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<ul style="list-style-type: none"> Retain the note as part of the record of personal health information about the individual that it has in its custody or under its control unless the custodian reasonably believes that the use or disclosure of personal health information will not have an adverse impact as described in Section 15. 				
<p>Ensure that for personal health information to be disclosed outside of Newfoundland and Labrador, the following circumstances exist:</p> <p>(a) the individual who is the</p>				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>subject of the information consents to the disclosure;</p> <p>(b) the disclosure is permitted by this Act or the regulations;</p> <p>(c) the person receiving the information performs functions similar to the functions performed by a person to whom this Act would permit the custodian to disclose the information in the province under subsection 40(2);</p> <p>(d) the following conditions are met:</p> <p>(i) the disclosure is for the purpose of health planning or health administration,</p>				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>(ii) the information relates to health care provided in the province to a person who is a resident of another province or territory of Canada , and</p> <p>(iii) the disclosure is made to the government of that other province or territory of Canada ;</p> <p>(e) the disclosure is reasonably necessary for the provision of health care to the individual and the individual has not expressly instructed the custodian not to make the disclosure in its entirety; or</p> <p>(f) the disclosure is reasonably necessary for the administration of payments in connection with the</p>				

Requirement	Privacy Safeguards	Implementation		Effectiveness
provision of health care to the individual or for contractual or legal requirements in that connection.				
When personal health information disclosure has been limited at the request of the individual, inform the individual to whom the information is disclosed of the limitation.				

Principle 6 – Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Requirement	Privacy Safeguards	Implementation		Effectiveness
Take reasonable steps to ensure that the personal information is accurate, complete and up-to-date.				
When information is shared or disclosed, establish procedures to provide notices of correction, either automatically or at the request of an individual.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Record and retain requests for a review of errors or omissions and corrections or decisions not to correct.</p> <p>NOTE: This requirement also dealt with under Principle 9, Individual Access, below.</p>				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Establish a clearly defined process by which an individual may request access to, assess and discuss or dispute the accuracy of his or her personal health information or record.</p> <p>NOTE: This requirement also dealt with under Principle 9, Individual Access, below.</p>				

Principle 7 – Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Ensure that there are practices, policies and procedures in place to, at a minimum:</p> <ul style="list-style-type: none"> • protect the confidentiality of personal health information that is in its custody or under its control and the privacy of the individual who is the subject of that information; • restrict access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that 				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the information was collected or will be used;</p> <p>protect the confidentiality of personal health information that will be stored or used in a jurisdiction outside the province or that is to be disclosed by the custodian to a person in another jurisdiction and the privacy of the individual who is the subject of that information; and</p> <p>Provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information.</p>				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<ul style="list-style-type: none"> Be stored or used in a jurisdiction outside the province or that is to be disclosed by the custodian to a person in another jurisdiction and the privacy of the individual who is the subject of that information; and Provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information. 				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Take steps that are reasonable in the circumstances to ensure that:</p> <ul style="list-style-type: none"> Personal health information in the custodian's custody or control is protected against theft, loss and unauthorized access, use or disclosure; Records containing personal health information in the custodian's custody or control are protected against unauthorized copying or modification; and Records containing personal health information in the custodian's custody or control are retained, transferred and disposed of in a secure manner. 				
	Version []			B-30

Requirement	Privacy Safeguards	Implementation		Effectiveness
Ensure that employees, agents, contractors and volunteers, and those health care professionals who have the right to treat persons at a health care facility operated by the custodian, are aware of the duties imposed by PHIA and the regulations and by the custodian's information policies and procedures referred to in Part II, Section 13.				
Establish processes for notifying the Commissioner of a material breach involving the unauthorized collection, use, or disclosure of personal health information.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
Establish processes for notifying the individual(s) affected of a material breach involving the unauthorized collection, use, or disclosure of personal health information; or if the personal health information is stolen, lost, disposed of in a manner other than those permitted under PHIA or disclosed to or accessed by an unauthorized person.				

Principle 8 – Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Requirement	Privacy Safeguards	Implementation		Effectiveness
Make available to those who are or who are likely to be affected by the custodian's activities a written statement that provides a general description of the custodian's information policies and procedures.				
Establish procedures for notifying individuals whose personal health information is stolen, lost, disposed of in a manner other than permitted by PHIA or the regulations, or disclosed to or accessed by an unauthorized				

Requirement	Privacy Safeguards	Implementation		Effectiveness
person.				
Inform the Commissioner in the event of a material breach.				

Principle 9 – Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Establish procedures and ways that allow the individual who is the subject of the information to request access to his or her personal information.</p> <p>NOTE: The exceptions to an individual's right of access are set out in section 58 of PHIA.</p>				

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Formal procedures for access must include the following elements:</p> <ul style="list-style-type: none"> • Assistance to individuals whose requests that do not contain enough detail (Section 54); • Quick response time to requests; time is not to exceed 60 days (Section 55); • Record availability and copies of records (Section 56); • Fees (Section 57); • Ensuring the retention of information subject to a request until access is provided or denied (Part II, Section 15); and • Refusal of access (Section 58). 				
	Version []			B-36

Requirement	Privacy Safeguards	Implementation	Effectiveness
<p>Establish a process for correcting information on request that includes the following elements:</p> <ul style="list-style-type: none"> • Examination of the request to ensure that the record is demonstrably incorrect or incomplete and supplies the necessary information for correction (Section 62); • Written notification to an individual requesting correction that a correction to his/her information has been made (Sections 60 and 63); • Notification of correction to other parties to which the original information was disclosed within 			

Requirement	Privacy Safeguards	Implementation	Effectiveness
<p>the past 12 months (Section 63);</p> <ul style="list-style-type: none"> • Corrections are made no later than 30 days following a request (Section 61). <p>NOTE: The exceptions to an individual's right of correction are set out in section 62 of PHIA.</p>			

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Make appropriate corrections to records of personal health information:</p> <ul style="list-style-type: none"> Record correct information in the record, and either strike out incorrect information without obliterating the record or label information as incorrect and sever it if striking out the information is not possible. Where it is not possible to record the correct information in the record, establish a practical system to inform a person accessing the record that the information in the record is incorrect and to direct the person to the correct information. 				

Requirement	Privacy Safeguards	Implementation		Effectiveness
Annotate records regarding refusals to correct personal health information, including details of the request, and notify the individual requesting the change regarding the annotation.				
Ensure that access to records for purposes of correction is provided only following confirmation of an individual's identity.				

Requirement	Privacy Safeguards	Implementation		Effectiveness
Establish processes for retaining personal health information that is the subject of a request for access under subsection 53(1) or for correction under subsection 60(1) for as long as necessary to allow the individual to exhaust any recourse under PHIA that he or she may have with respect to the request.				

Principle 10 – Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Requirement	Privacy Safeguards	Implementation		Effectiveness
<p>Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.</p> <p>NOTE: Part VI of PHIA provides for review of complaints by the Commissioner; Part VII addresses appeals.</p>				