Provincial Reportable Incident Response Process (PRIRP)

Version 1.1 (May 2019)

Table of Contents

Introduction

To ensure consistency and effectiveness of responses to health information under threat, Alberta Health has instituted the Provincial Reportable Incident Response Process (PRIRP for all health stakeholders managing or accessing Alberta's provincial Electronic Health Record (EHR) including its subsystems and repositories. This process covers incidents of data confidentiality, data integrity, and data availability and is divided into five phases.

PRIRP is applicable to all health stakeholders managing, accessing, or regulating Alberta's EHR including its subsystems and repositories.

- *Alberta Health*;
- *Alberta Health Services*;
- *Covenant Health*;
- *Community custodians*;
- *Other external stakeholders* such as the public, the *Alberta Medical Association*, and the colleges of regulated health professions;
- *Office of the Information and Privacy Commissioner of Alberta*.

Health stakeholders use PRIRP to report a suspected or known security incident to Alberta Health. Alberta Health will assess the threat from the incident, and if valid will assemble an Incident Response Team (IRT). The IRT will be led by the Alberta Health Security team and include the reporting health stakeholder(s) and other applicable resources for any particular incident. The IRT will communicate as needed with other stakeholders impacted by the incident.

Applying PRIRP

PRIRP applies to unauthorized disclosure, alteration, or loss of access to health information. Incidents may be simple or complex, may consist of individual or system-level exposure, and consist of one or more of the following.

- *Incident of Data Confidentiality*: An unauthorized viewing of patient records, or disclosures due to lost information stored on electronic media including the provincial EHR.

  A data confidentiality incident includes viewing health records of individuals that are not in a current care relationship with the user without written consent, or viewing records of public figures, celebrities, or the public at large without a need to know. There is no minimum number of unauthorized accesses that constitute data confidentiality incident; however the number of unauthorized accesses will determine the magnitude of the

response. Unintentionally accessing a single record by entering incorrect patient data is not considered to be a provincially reportable data confidentiality incident. Encrypted information that has been lost does not generally qualify as a data confidentiality incident as the information remains protected by encryption. However if concerns exist that **increase the risk of harm** such as weak encryption, or the number and/or type of records lost, then the incident is expected to be reported.

- *Incident of Data Integrity*: Any amount of incorrect or incomplete data appearing in, or flowing to, the provincial EHR system.

  A data integrity incident can be caused by system or human error. Any data integrity issue impacting patient safety is considered to be a reportable incident. The number and/or type of affected records may **increase the risk of harm** and determine the magnitude of the response. Triggers for PRIRP occur whenever there is a potential patient safety issue or a significant number records are affected. Normal data entry errors corrected by quality assurance processes do not constitute a data integrity incident.

- *Incident of Data Availability*: Any unscheduled period when the provincial EHR system is unavailable or information is lost.

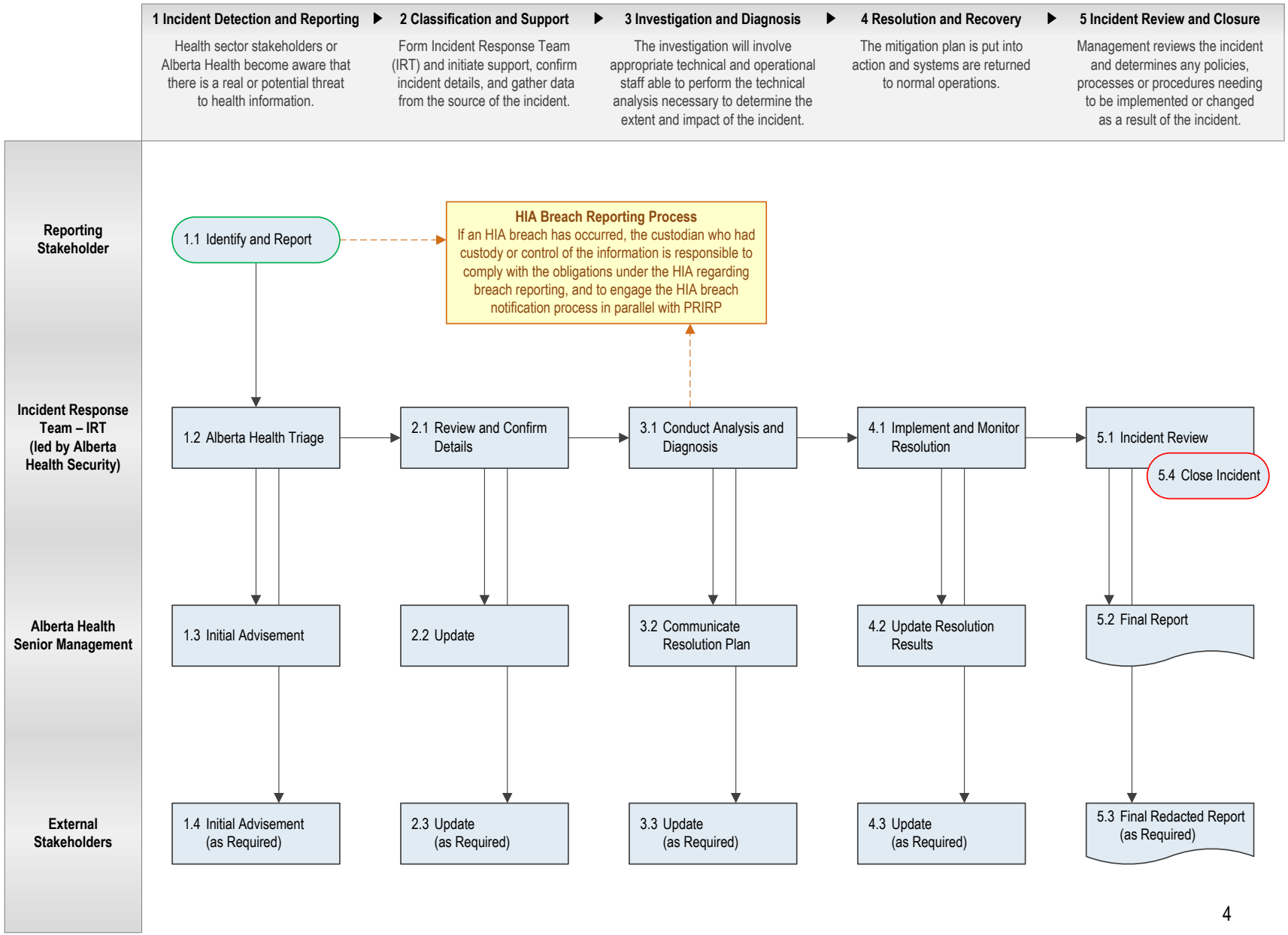
  Triggers for PRIRP include unplanned interruptions to provincial EHR systems with the potential to **increase the risk of harm** to public safety. These outages may result in initiation of business continuity or disaster recovery plans in the affected organization. Poor performance of provincial EHR systems is not considered a PRIRP trigger, but still may be investigated by Alberta Health and/or the Health stakeholder(s).

- *HIA Breach*: A loss of, unauthorized access to, or unauthorized disclosure of individually identifying health information in the custody or control of a custodian resulting in a risk of harm to an individual. If an HIA breach occurs, the custodian who had custody or control of the information is responsible to comply with the obligations under the HIA regarding breach reporting and to engage the HIA breach notification process in parallel with PRIRP.

  Alberta Health has released a variety of materials to provide information and guidance on the HIA breach notification requirements including Chapter 14: Duty to Notify of the *Health Information Act* Guidelines and Practices Manual. Additional information, including the form to be used for Notification to Alberta's Health Minister, is available from the *Health Information Act* section of Alberta Health's website.

PRIRP is designed to accommodate the uniqueness and complexity of incidents through the completion of all its five phases. Each phase consists of multiple steps and includes responsibilities to be completed by the identified health sector stakeholders. While the phases and steps are presented in an orderly fashion, there may be overlap during execution of PRIRP. The phases and steps are summarized in the diagram on page 4 and described in detail starting on page 5.

Provincial Reportable Incident Response Process



1 Incident Detection and Reporting

Health sector stakeholders or Alberta Health become aware that there is a real or potential threat to health information.

1.1 Identify and Report

Reporting stakeholders with a reasonable suspicion that there is a real or potential threat to health information are expected to include PRIRP within their organization's existing incident response processes. The stakeholder reports the incident to Alberta Health using the PRIRP form, Appendix A.

If an HIA breach has occurred, the custodian who had custody or control of the information is responsible to comply with the obligations under the HIA regarding breach reporting (see page 3), and to engage the HIA breach notification process in parallel with PRIRP.

Similarly, health sector stakeholders discovering a real or potential threat to health information outside of their responsibilities for custody or control, are expected to notify the appropriate custodian and to use the HIA breach notification process in parallel with PRIRP (see page 3) to notify Alberta Health.

1.2 Alberta Health Triage

Upon receipt of real or potential threat to health information, Alberta Health Security initiates PRIRP by recording the incident and assigning an IRT lead.

1.3 Initial Advisement to Alberta Health Senior Management

The IRT lead uses Alberta Health's internal reporting processes to provide an initial advisement to Alberta Health senior management with an early indication of potential threat to health information.

1.4 Initial Advisement to External Stakeholders

The IRT lead, upon direction from Alberta Health senior management in 1.3, includes consideration of the severity of the potential or real threat and may provide early indication to external stakeholders such as Office of Information and Privacy Commissioner (OIPC).

2 Classification and Support

Form Incident Response Team (IRT) and initiate support, confirm incident details, and gather data from the source of the incident.

2.1 Review and Confirm Details

The IRT lead identifies and mobilizes additional IRT members to review and confirm incident details, to gather any additional information required from the incident source, and to identify an incident owner.

2.2 Update to Alberta Health Senior Management

The IRT lead updates Alberta Health senior management with the incident details and next steps.

2.3 Update to External Stakeholders as Required

The IRT lead, upon direction from Alberta Health senior management in 2.2, provides an update to external stakeholders as required.

3 Investigation and Diagnosis

The investigation will involve appropriate technical and operational staff able to perform the technical analysis necessary to determine the extent and impact of the incident.

3.1 Conduct Analysis and Diagnosis

IRT members will conduct analyze and diagnose activities in parallel with any investigations initiated by the incident owner. The goal is to understand the cause of the incident, identify any impacts to health or other confidential information. The IRT lead and incident owner are expected to keep each other informed on progress. IRT members further develop and identify a resolution plan as required.

Should additional security incident details be gathered which confirm the occurrence of an HIA breach, the custodian who had custody or control of the information is responsible to comply with the obligations under the HIA regarding breach reporting (see page 3), and to engage the HIA breach notification process in parallel with PRIRP.

3.2 Communicate Resolution Plan to Alberta Health Senior Management

The IRT lead will inform Alberta Health senior management of the results of the investigation and provide details on the resolution plan.

3.3 Update to External Stakeholders as Required

The IRT lead, upon direction from Alberta Health senior management in 3.2, provides an update to external stakeholders as required.

4 Resolution and Recovery

The resolution plan is put into action and systems are returned to normal operations.

4.1 Implement and Monitor Resolution

The IRT lead works closely with the incident owner and any identified health sector stakeholders to implement the resolution plan and to monitor that systems return to normal operational status as expected.

4.2 Advise Resolution Results to Alberta Health Senior Management

The IRT lead will provide Alberta Health senior management with the results of the resolution plan implementation across all organizations involved.

4.3 Update to External Stakeholders as Required

The IRT lead, upon direction from Alberta Health senior management in 4.2, provides an update to external stakeholders as required.

5 Incident Review and Closure

IRT reviews the incident and makes recommendations to involved parties.

5.1 Incident Review

The IRT reviews the incident including reporting, response, causes, and the resolution; and considers these in identifying policy, process, procedures, or measures needing to be implemented or changed.

5.2 Final Report to Alberta Health Senior Management

The IRT lead is responsible to submit a final report to Alberta Health senior management documenting the PRIRP event and includes IRT identified recommended changes. The report may contain sensitive information and will be restricted to Alberta Health senior management and other parties directly involved with the incident.

5.3 Final Redacted Report to External Stakeholders as Required

The IRT lead, upon direction from Alberta Health senior management in 5.2, redacts sensitive information in the preparation and sharing of a final report, as required, with external stakeholders.

5.4 Formally Close Incident

The IRT lead formally disbands the IRT and closes the PRIRP incident.

Document History

Version	Changes	Author
1.0 (Aug 2005)	Initial Document	AHW Privacy and Security
1.01 (Feb 2007)	Updated for Pharmacy incident	AHW IPC
1.02 (Oct 2009)	Refresh	AHW ICA Unit
1.03 (Mar 2013)	Branding updated	Alberta Health Security Team
1.1 (Oct 2018)	Updated for HIA Breach	Alberta Health Privacy and Security Team
1.1 (May 2019)	Updated reporting form	Alberta Health Privacy and Security Team

Appendix A: Provincial Reportable Incident Response Process Form

Form available from *http://www.albertanetcare.ca/learningcentre/documents/PRIRP-Form.pdf*

Appendix A: Provincial Reportable Incident Response Process Form

This form is used to engage the Provincial Reportable Incident Response Process (PRIRP). The form is to be updated and submitted as the appropriate information is gathered concerning the incident for each of the five phases of PRIRP. Do not include health information or sensitive information when completing this form. Submit completed form to AH.Security@gov.ab.ca.

If you have, any questions call the *EHR Helpdesk at* **1.877.931.1638** or contact the Alberta Health Security Team at **780.643.9343**.

Phase 1 Incident Detection and Reporting
Reporting stakeholders with a reasonable suspicion of a real or potential threat to health information are to complete and submit Phase 1 of the form. Breaches of health information should also refer to HIA Breach Reporting requirements identified on page 3 of PRIRP.

Reporting Stakeholder Details / Identify and Report (PRIRP 1.1)

Date of Incident:
Full Name: Click or tap here to enter text.
Organization: Click or tap here to enter text.
Job Title: Click or tap here to enter text.
Phone Number: Click or tap here to enter text.
Email Address: Click or tap here to enter text.

Incident Information
Include description of threat (what type of health information has been disclosed, accessed inappropriately, lost or stolen, estimates on number of records or individuals impacts, when the threat was discovered, how long the threat has existed, and any other relevant details.
Click or tap here to enter text.

Phase 2 Classification and Support
Complete and submit as directed by PRIRP Incident Response Team (IRT) Lead with updated information gathered from incident source.

Review and Confirm Details (PRIRP 2.1)
Confirm incident details and include any updated information from the source of the incident. Include details information on any containment steps taken.
Click or tap here to enter text.

Phase 3 Investigation and Diagnosis
Complete and submit as directed by PRIRP IRT Lead with information gathered from technical and operational sources.

Analysis and Diagnosis Update (PRIRP 3.1)
Include technical and operational analysis and diagnostic updates from any parallel incident owner investigation, what is known about cause of the incident, and any identified impacts to health or other confidential information.
Click or tap here to enter text.

Phase 4 Resolution and Recovery
Complete and submit as directed by PRIRP IRT Lead with information gathered from resolution activities.

Implementation and Monitoring Update (PRIRP 4.1)
Include updates regarding resolution plan, testing of resolution, and system monitoring results.
Click or tap here to enter text.

Phase 5 Incident Review and Closure
PRIRP IRT Lead completes with information gathered from resolution activities; used to make recommendations to involved parties.

Incident Review (PRIRP 5.1)
Review details provided in above phases to identify policy, process, procedures, or measures needing to be implemented or changed.

Click or tap here to enter text.