Integrated Incident Management Process

Integrated Assessment Record (IAR)

Version 3.2

August, 2011

Table of Contents

Introduction

Incident Management is the ability to provide end to end management of a series of events that are initiated in response to a Privacy or Security breach.

The Integrated Assessment Record (IAR) integrated incident management process deals with IAR-related privacy and security incidents in a coordinated fashion. Incidents that affect multiple participating organizations will involve both the Health Information Network Provider (HINP) and the affected Health Information Custodians (HICs); as well as the privacy officers at the HINP and the participating organizations.

An incident is the contravention of a policy, procedure, duty or contract, or a situation of interest that results in the potential exposure of sensitive information to unauthorized parties. Each participating organization will use its existing incident management processes to handle incidents.

The following is a sample of privacy and security incidents that may occur in IAR:

- Printed patient assessment information is left in a public area (e.g. Tim Horton)
- Theft, loss, damage, unauthorized destruction or modification of patient records
- Inappropriate access of patient information by unauthorized users
- Large amount of IAR records were accessed by a single individual in a short period of time (out of the ordinary)
- User account and password was compromised
- Network infrastructure is attacked by hackers
- Violation of joint security and privacy policies or procedures

The Information & Privacy Commissioner (IPC) recommends that the HINP develops a privacy breach protocol to handle any potential privacy breach incident. The protocol enables the HINP and participating organizations to respond quickly and in a coordinated way during a privacy breach. The protocol also defines the roles and responsibilities of each party in this integrated environment, to ensure that investigation and containment are more effective and efficient, and remediation easier to implement.

Incidents can originate from the HIC or the HINP. An incident can also be reported by the clients or a 3rd party of a HIC, or a 3rd party to the HINP.

Following are the four scenarios described in this document.

Scenario 1 – Incident detected by the HIC

- Printed patient assessment records lost
- User account and password compromised
- Network at HIC broken into by hackers (suspect IAR upload files have been accessed)

Scenario 2 – Incident reported by client or 3rd party to the HIC

- Client reports: "My ex-spouse working in your organization accessed my medical information and used it in our child custody case. Why can he/she access my medical records?"
- Someone (non-patient) found printed patient assessment information on HIC letterhead left at Tim Hortons

Scenario 3 – Incident detected by the HINP

- IAR backup data unaccounted for (loss or stolen)
- IAR database hacked into by hackers
- Large amount of IAR records were accessed by a single individual in a short period of time (out of the ordinary)
- Missing data backup tape that contains server and system data, but no personal health information (PHI)

Scenario 4 – Incident reported by 3rd party to the HINP

- Record management service provider reports to HINP that one IAR data backup tape went missing during transit
- Missing data backup tape that contains server and system data, but no PHI

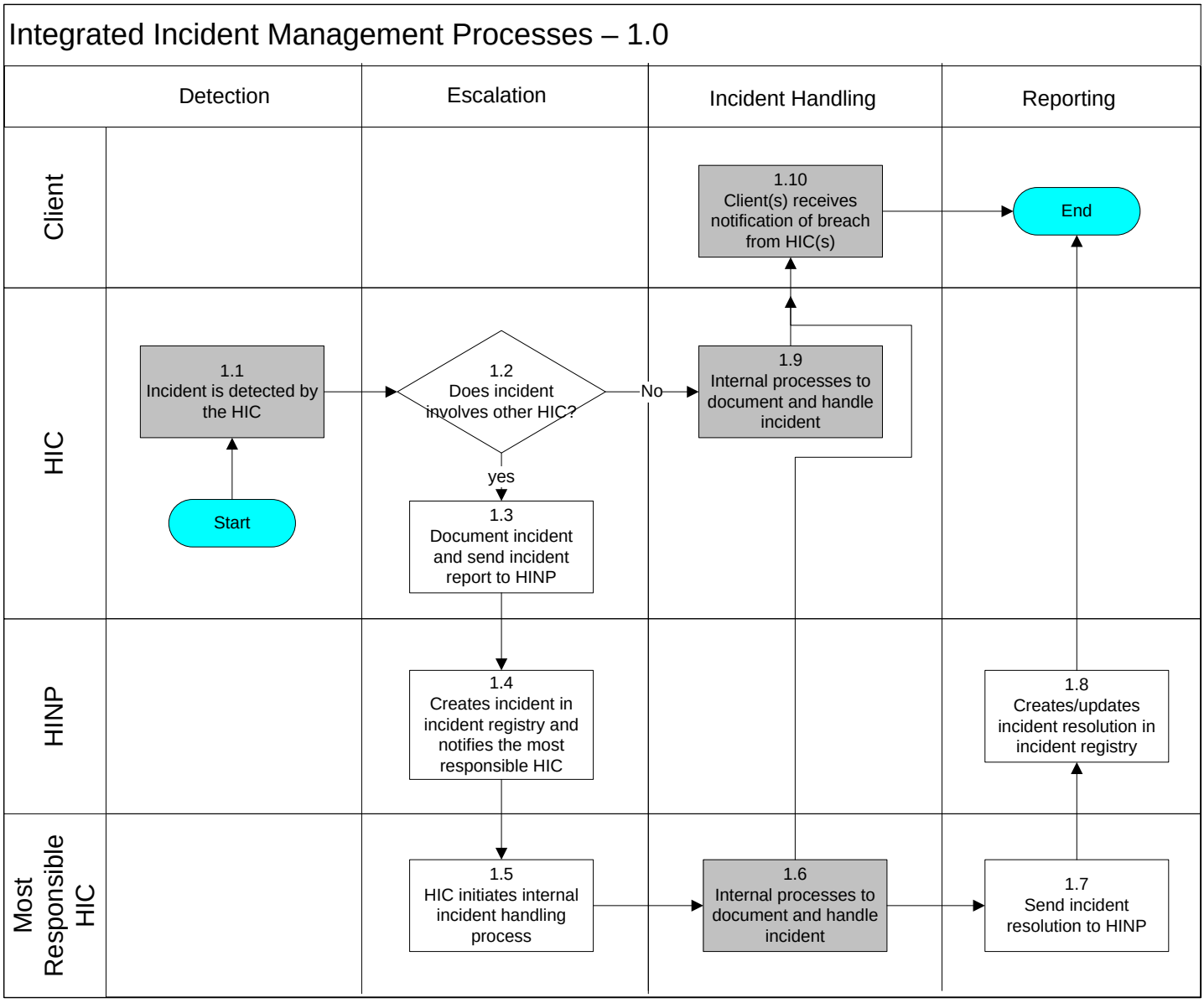
Notification of Clients

PHIPA requires the Health Information Custodian to notify the clients if there is a privacy breach that involves their personal health information. In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach concerning his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in order to develop the best notification approach to the client. This notification can be in the form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

This document translates the above scenarios into defined processes and steps as it relates to the Integrated Assessment Record. It identifies responsibilities and delineates between those tasks which should already be in place within any given Health Information Custodian and those tasks which are introduced with the IAR.

Processes

Scenario 1 – Incident Detected by HIC



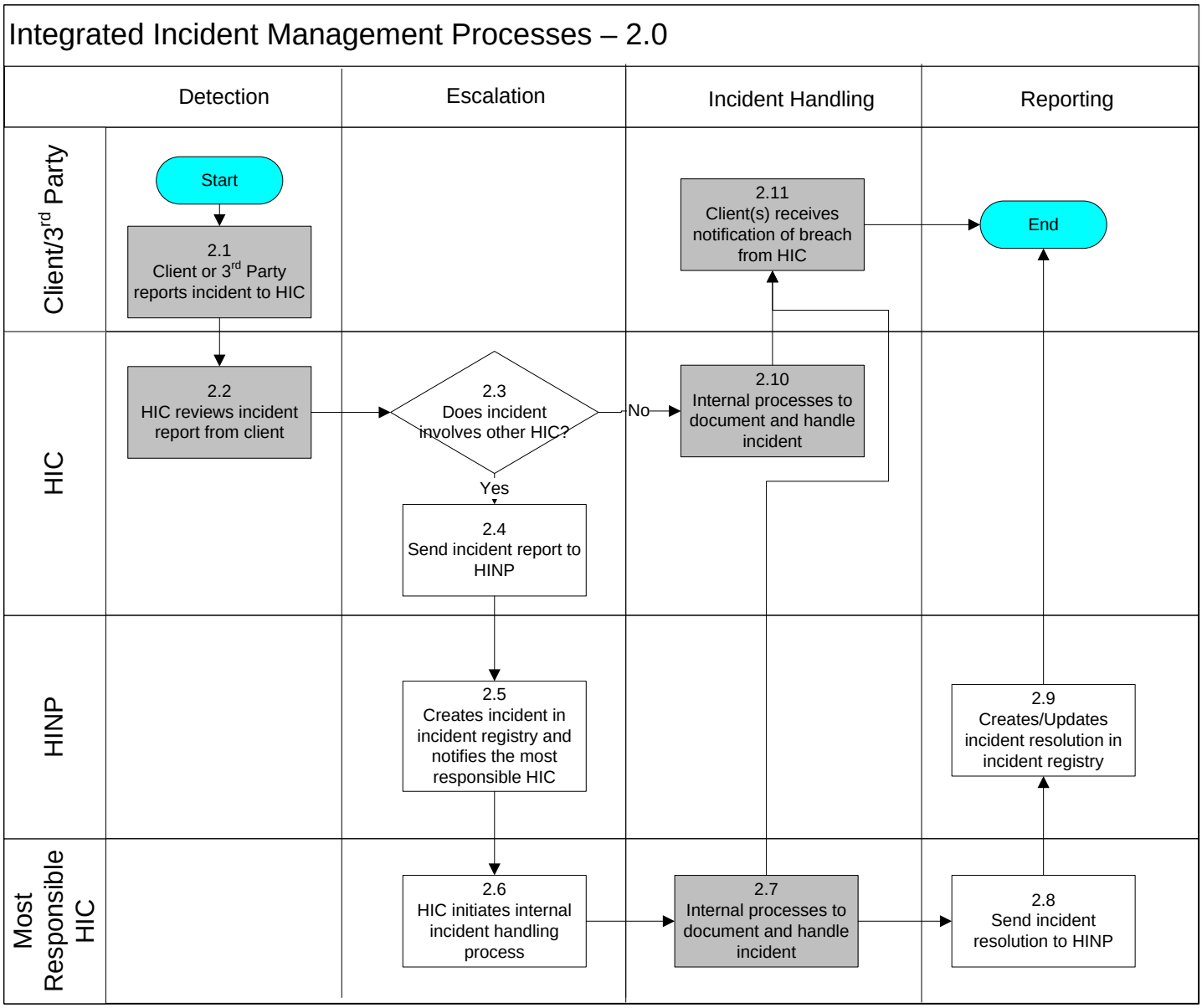
**Note:* *Shaded boxes indicate steps or tasks which should currently exist within the Health Information Custodian and Health Information Network Provider. Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR.*

Ref No.	Task / Step	Owner	Artifacts
	Integrated Incident Management Process – Scenario 1 Incident detected by HIC Sample scenarios: • Printed patient assessment records were lost • User account and password were compromised • IAR upload files have been compromised possibly by hackers breaking in to network at participating organization (HIC)		
1.1	The incident is detected by the normal incident detection and monitoring process at the HIC or staff at HIC reports incident internally to HIC privacy officer.	Health Information Custodians	Incident Report
1.2	HIC privacy officer triages the reported/detected incident - containment is the first priority - and determines if the incident involves other participating organizations/HICs. • If incident involves other HICs, then the HIC sends the Incident Report to the HINP. (Ref 1.3) • If incident involves only the local HIC, then the HIC initiates internal incident management process. (Ref 1.9) *The HIC has to notify the HINP within 24 hours of receiving the Incident Report if the incident is determined to affect other HICs in accordance with the Data Sharing Agreement*	Health Information Custodians	
1.3	HIC privacy officer documents the incident and sends the Incident Report to the HINP.	Health Information Custodians	Incident Report
1.4	HINP creates incident in the Incident Registry and notifies the most responsible HIC about the incident.	Health Information Network Provider	Incident Report and Incident Registry
1.5	The most responsible HIC initiates internal processes to handle the reported/detected incident.	Health Information Custodians	
1.6	HIC executes the internal incident handling process and documents the incident.	Health Information Custodians	
1.7	HIC sends the incident resolution detail to the HINP.	Health Information Custodians	Updated Incident Report

1.8	HINP creates or updates Incident Record with the resolutions in the Incident Registry.	Health Information Network Provider	Incident Registry
1.9	HIC initiates internal processes to document and handle the reported/detected incident.	Health Information Custodians	
1.10*	Client receives notification from HIC regarding the privacy breach of their respective record(s). This is part of the HIC's internal incident handling procedure.	Health Information Custodians	

*Note: In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach concerning his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in order to develop the best notification approach to the client. This can be in a form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

Scenario 2 – Incident Detected by Client or 3rd Party of HIC



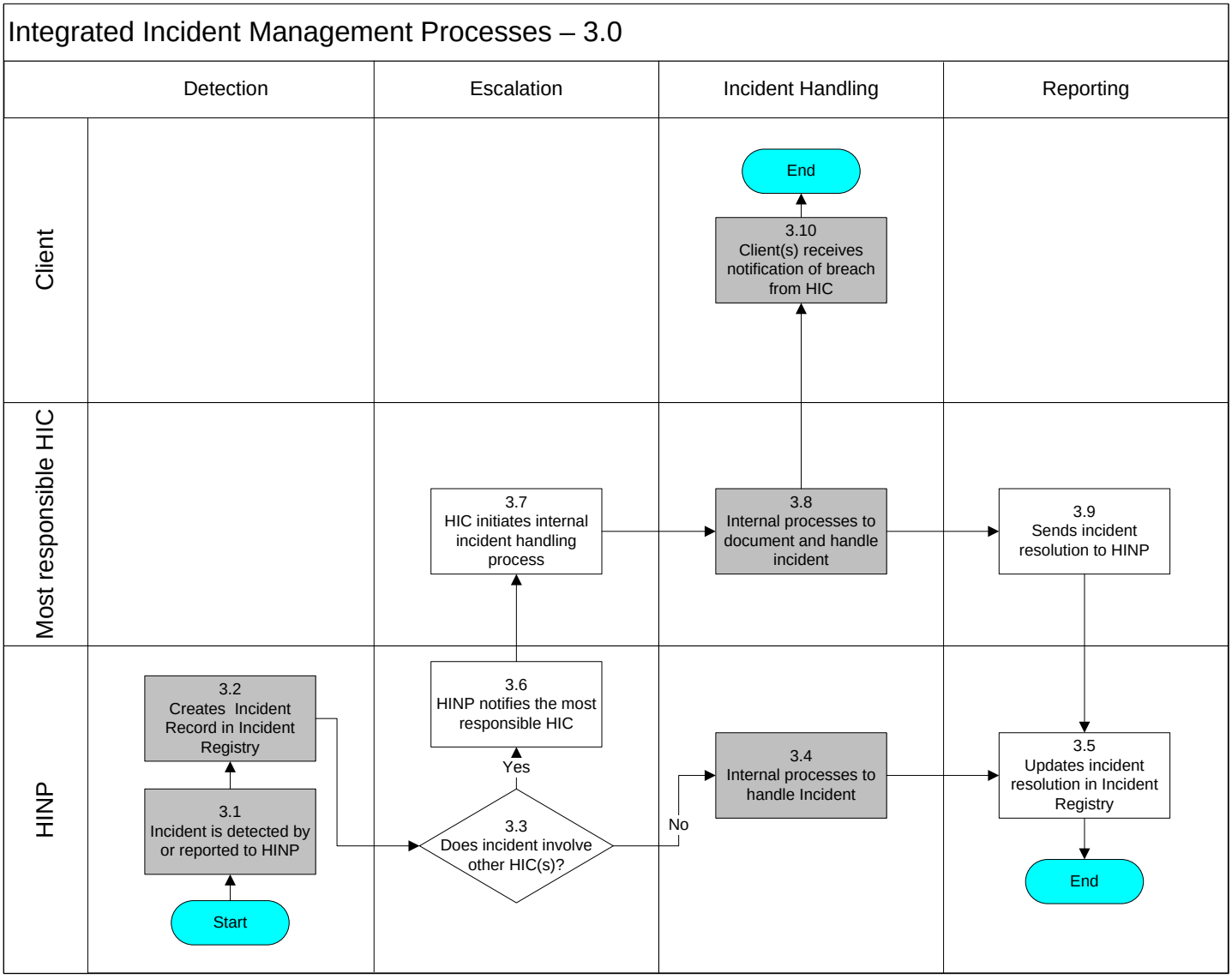
**Note:* *Shaded boxes indicate steps or tasks which should currently exist within the Health Information Custodian and Health Information Network Provider. Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR.*

Ref No.	Task / Step	Owner	Artifacts
	Integrated Incident Management Process – Scenario 2 Incident reported by client Sample scenarios: • A client of a HIC finds out his/her ex-spouse working at the HIC accessed his/her medical information and used it in his/her child custody case. He/she is wondering why ex-spouse can access his/her medical record for such a purpose.		
2.1	Clients or 3rd party contacts HIC privacy officer, or other HIC staff, to report the incident.	Health Information Custodian	Incident report
2.2	HIC Privacy Officer reviews the Incident Report received (containment is the first priority) from client or internal staff.	Health Information Custodian	Incident report
2.3	HIC Privacy Officer triages the reported incident, and determines if the incident involves any other participating organizations/HICs. • If incident involves other HICs, then the HIC sends the incident report to the HINP. (Ref 2.7) • If incident involves only the local HIC, then the HIC initiates the internal incident management process. (Ref 2.4) *The HIC has to inform the HINP within 24 hours of receiving the Incident Report if the incident is determined to affect other HICs in accordance with the Data Sharing Agreement*	Health Information Custodians	
2.4	HIC sends Incident Report to HINP	Health Information Custodians	Incident Report
2.5	HINP creates incident in the Incident Registry and notifies the most responsible HIC about the incident.	Health Information Network Provider	Incident report
2.6	The most responsible HIC initiates internal processes to handle the reported/detected incident.	Health Information Custodians	
2.7	HIC executes the internal incident handling processes and documents the incident.	Health Information Custodians	

2.8	HIC sends the incident resolution detail to the HINP.	Health Information Custodians	Updated incident report
2.9	HINP creates or updates Incident Registry with details of incident resolution.	Health Information Network Provider	Incident Registry
2.10	HIC initiates internal processes to document and handle the incident.	Health Information Custodians	
2.11*	Client receives notification from HIC regarding the privacy breach of their respective record(s). This is part of the HIC's internal incident handling procedure.	Health Information Custodians	

*Note: In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach of his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in order to develop the best notification approach to the client. This can be in a form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

Scenario 3 – Incident Reported by the HINP



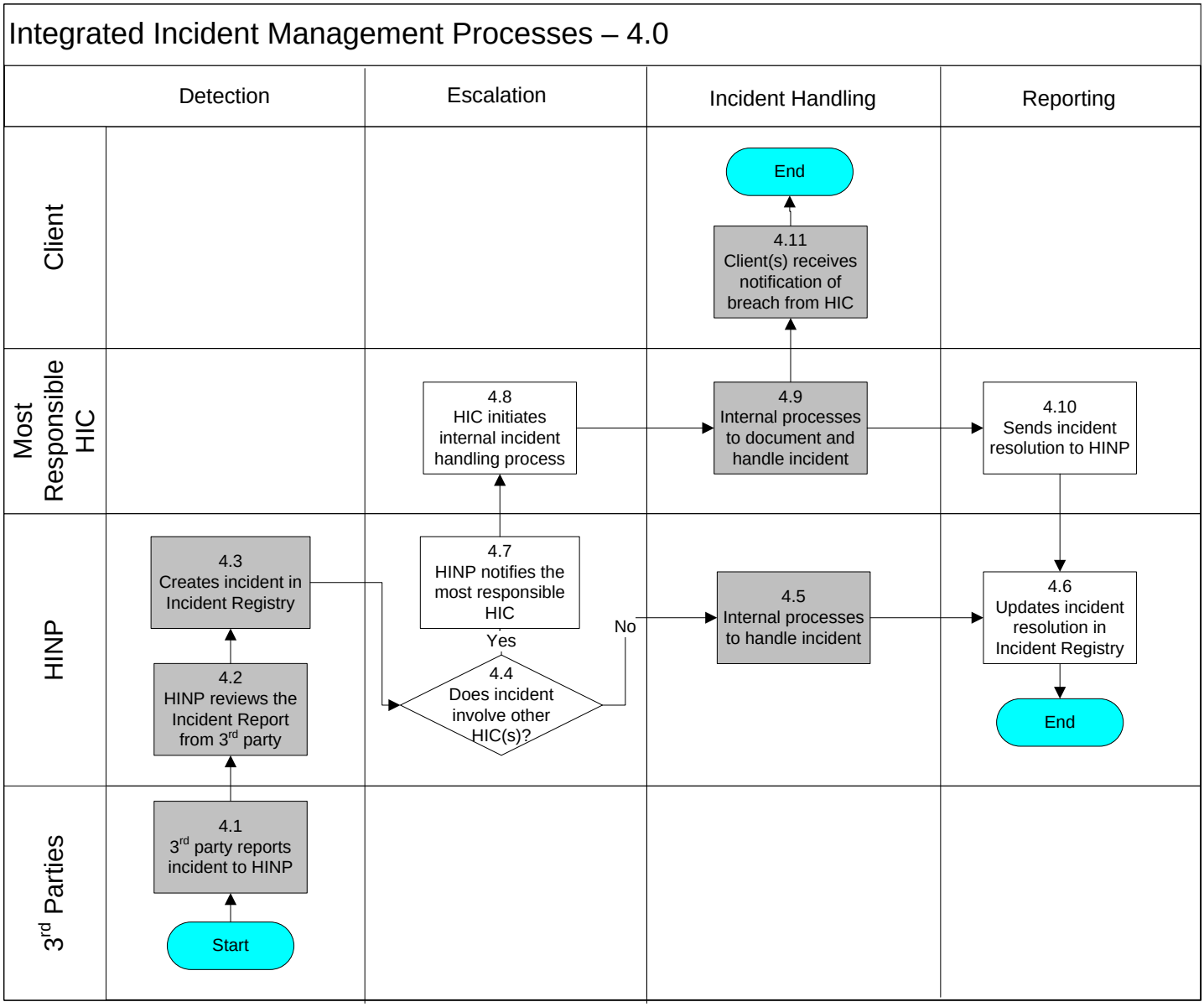
**Note:* *Shaded boxes indicate steps or tasks which should currently exist within the Health Information Custodian and Health Information Network Provider. Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR.*

Ref No.	Task / Step	Owner	Artifacts
	Integrated Incident Management Process – Scenario 3 Incident detected by HINP Sample scenarios: • IAR backup data unaccounted for (lost or stolen) • IAR database was hacked into by hackers • Large amount of IAR records were accessed by a single individual in a short period of time (duration out of the ordinary) • Missing data backup tape contains server and systems information only (no PHI)		
3.1	The incident is detected by the normal incident detection and monitoring process at the HINP, or staff at HINP reported incident internally to HINP privacy officer.	Health Information Network Provider	Incident Report
3.2	HINP keeps track of incidents by creating a record in the Incident Registry.	Health Information Network Provider	Incident Registry
3.3	HINP Privacy Officer triages the reported/detected incident, and determines if the incident involves other participating organizations/HICs. • If incident involves other HICs, then the privacy officer notifies the most responsible HIC. (Ref 3.6) • If incident involves only the HINP, then the privacy officer initiates the internal incident management process. (Ref 3.4) *The HINP has to inform the affected HIC within 24 hours of receiving the Incident Report in accordance with the Data Sharing Agreement.*	Health Information Network Provider	
3.4	HINP executes internal processes to handle the reported/detected incident.	Health Information Network Provider	
3.5	HINP updates Incident Registry with details of incident resolution.	Health Information Network Provider	Incident Registry
3.6	HINP notifies the most responsible HIC about the incident. If applicable, the HINP continues to investigate and contain the incident, and provides all supporting information to assist the internal incident handling at the HIC.	Health Information Network Provider	Incident Report

3.7	The most responsible HIC initiates the internal incident handling process.	Health Information Custodians	
3.8	The HIC executes internal processes to document and handle the reported/detected incident.	Health Information Custodians	
3.9	The HIC sends incident resolution details to the HINP.	Health Information Custodians	Updated incident report
3.10*	Client receives notification from HIC regarding the privacy breach of their respective record(s). This is part of the HIC's internal incident handling procedure.	Health Information Custodians	

*Note: In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach of his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in order to develop the best notification approach to the client. This can be in a form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

Scenario 4 – Incident Reported by 3rd Party to HINP



*Note: *Shaded boxes indicate steps or tasks which should currently exist within the Health Information Custodian and Health Information Network Provider. Non-shaded boxes indicate steps which are being introduced with the implementation of the IAR.*

Ref No.	Task / Step	Owner	Artifacts
	Integrated Incident Management Process – Scenario 4 Incident reported by 3rd party of HINP Sample scenarios: • Record management service provider reports to HINP that one IAR backup data tape went missing during transit • Missing data backup tape contains server and systems information only (with no PHI)		
4.1	3rd party reports incident to HINP.	Health Information Network Provider	Incident report form
4.2	HINP Privacy Officer reviews the received Incident Report from 3rd party.	Health Information Network Provider	
4.3	HINP creates incident in incident registry.	Health Information Network Provider	Incident Registry
4.4	HINP Privacy Officer triages the reported incident, and determines if the incident involves other participating organizations/HICs. • If incident involves other HICs, then the HINP privacy officer notifies the most responsible HIC about the incident. (Ref 4.7) • If incident involves only the HINP, then the HINP initiates the internal incident management process. (Ref 4.5) *The HINP has to inform the other affected HICs within 24 hours of receiving the Incident Report if the incident is determined to affect other HICs in accordance with the Data Sharing Agreement*	Health Information Network Provider	
4.5	HINP initiates internal processes to handle the reported incident.	Health Information Network Provider	
4.6	HINP updates the incident resolution detail in the Incident Registry.	Health Information Network Provider	Incident Registry
4.7	HINP notifies the most responsible HIC.	Health Information Network Provider	Incident report

4.8	The most responsible HIC initiates internal processes to handle the reported/detected incident.	Health Information Custodians	
4.9	The HIC executes the internal processes to document and handle the incident.	Health Information Custodians	
4.10	The HIC sends the incident resolution detail to the HINP.	Health Information Custodians	Updated incident report
4.11*	Client receives notification from HIC regarding the privacy breach of their respective record(s). This is part of the HIC's internal incident handling procedure.	Health Information Custodians	

*Note: In a situation where multiple HICs are investigating an incident that may affect the same client, the HINP privacy officer is to coordinate the notification to the client, in order to avoid the client receiving multiple notifications from different HICs regarding a privacy breach of his/her personal health information. The HINP privacy officer will facilitate among the various HICs involved in order to develop the best notification approach to the client. This can be in a form of a joint notification letter, or the HIC that is most responsible for the incident will take the lead to notify the client.

Appendix A – Incident Report Template for HIC

Integrated Assessment Record (IAR) System Incident Report **Fax No:**		
1. Contact Information *To be completed by the individual submitting this report*		
First Name	Last Name	Date (dd/mm/yyyy)
Email	Organization	
Phone No.	Title / Position	
Address (street, city, province, postal code)		
2. Incident Description *Describe the incident below.*		
Date of Incident (dd/mm/yyyy)	Involves PHI?	Reported By
Description / Details		
		Date of Incident (dd/mm/yyyy)
3. Incident Management		
Incident #	Internal Reference #	
Assigned to	Incident Receipt Date (dd/mm/yyyy)	
Containment Action		
Follow-up Action	Most Responsible (Primary) Organization	
Follow-up Date (dd/mm/yyyy)	Other Organizations (if any)	
Resolution Status		
Resolution Date (dd/mm/yyyy)		
Notes		

Appendix B – Incident Update Report Template for HIC

Integrated Assessment Record (IAR) System **Incident Update** **Fax No:**		
1. Contact Information *To be completed by the individual submitting this update*		
First Name	Last Name	Date (dd/mm/yyyy)
Email	Organization	
Phone No.	Title / Position	
2. Incident Information		
Incident #	Internal Reference #	
Client Contacted?	Date of Contact	
Update		
Notes		

Appendix C - IAR Centralized Incident Registry Template

Incident #	Reported By	Incident Date (dd/mm/yyyy)	Most Responsible (Primary) Org	Secondary Orgs	PHI Involved? (Y/N)	Actions Taken	Action Dates (dd/mm/yyyy)	Is client notified of incident? (Y/N)	Incident Resolution Status	Incident Resolution Dates (dd/mm/yyyy)
ABCD-1234	John Smith	13/05/2010	HIC A	HIC C HIC W HIC Z		Notified Secondary Orgs			Rejected/Resolved/Arbitration	