Theft, Fraud, Corruption, and Extortion

1. Introduction

1.1. Purpose

This policy outlines Providence Health Care's (PHC) commitment to maintaining a corporate culture that does not tolerate Theft, Fraud, Corruption, and/or Extortion.

PHC requires all Individuals associated with PHC to act, and be seen to act, with honesty and integrity in all matters related to PHC.

Individuals associated with PHC must not engage in acts of dishonesty or commit Theft, Fraud, Corruption, Extortion, or willful destruction of PHC property, or that of a client, resident or patient.

This policy:

- Describes PHC principles and expectations around Theft, Fraud, Corruption and/or Extortion;
- Describes how suspected Irregularities will be reported;
- Defines the process and the assignment of responsibilities for the escalation; investigation; and follow-up and mitigation of future incidents of allegations of Theft, Fraud, Corruption and/or Extortion;
- Outlines responsibilities for, the development, implementation and operations of a Fraud Risk Management framework at PHC.

1.2. Scope

This policy applies to **all** Individuals associated with PHC. See definitions section 6 below.

This policy does not replace, supersede, or seek to circumvent other processes, policies, or reporting obligations mandated in law.

1.3. Exceptions

This policy does not cover the following matters:

- Matters related to the reporting and correction of safety hazards and unsafe conditions made in accordance with the provisions of WorkSafe BC's Occupational Health and Safety Regulations (these should be reported using the process described in the Incident Reporting for Employees policy);
- Matters related to discrimination or harassment based on prohibited grounds as identified in BC's Human Rights Code and regulations (these should be reported using the process described in the Respect at Work policy);
- Matters related to the safe care of Patients, Clients, or Residents of PHC (these should be reported using the process described in the Safe Reporting policy).

2. Policy

Providence Health Care does not tolerate Theft, Fraud, Corruption, and/or Extortion. (These terms are defined in Section 6 below).

2.1 Process

Appendix A sets out the process that will be followed when there is a suspected incident of Theft, Fraud, Corruption and/or Extortion.

The PHC Cyber Extortion playbook and Cybercrime process map will set out the process that will be followed when there is a suspected incident of Cybercrime.

Note: Individuals must not pay any Ransom demands or contact law enforcement except as directed by this Policy.

2.1.1. Identifying and Reporting an Irregularity

Any Individual with specific knowledge or reasonable suspicion of an Irregularity must immediately report that Irregularity to:

1. The anonymous Safe Reporting Line at 604-806-9809 or by emailing PHC PHCSafeReport@vch.ca; or
2. Their direct supervisor/leader/management; or
3. Member of the senior leadership team; or
4. Internal Audit Offices at 604-875-4448 or by emailing InternalAuditServices@vch.ca.

In addition, Irregularities identified in cyberspace should be immediately notified to: cyberincident@phsa.ca.

Reports of Irregularities submitted pursuant to this policy must be made in good faith and must be based on reasonable grounds. Individuals who are found to have reported an Irregularity in bad faith or with malicious intent, will be subject to appropriate action which may include disciplinary and/or administrative measures up to and including termination of employment or termination of contractual relationships.

PHC will neither take nor permit any detrimental, negative consequence or retaliation (collectively "Retaliatory Action") against any Individual who reports in good faith; provides evidence of an Irregularity; or investigates an Irregularity.

Any Retaliatory Action taken against an Individual reporting in good faith will attract consequences including, if appropriate, disciplinary and/or administrative measures up to and including termination of employment or contractual relationships with PHC.

2.1.2. Reviewing a Report of an Irregularity

Upon receipt of a report of an Irregularity, the Human Resources (HR) partner (and leader/management, if appropriate[1]) will complete the initial assessment of the Irregularity. Once complete, the HR partner will the use the scenario and engagement checklist (see Appendix B) based on the type and severity of the Irregularity to determine who they will engage to lead and to otherwise participate in the investigation. In circumstances where medical staff are the subject of investigation, a representative from Medical Affairs will be included in the investigation team.

If the HR partner identifies a suspected Cybercrime that has not already been notified to Information Security Leadership (ISL), they will notify the ISL team by email at cyberincident@phsa.ca. Once the attack is a confirmed threat, the Incident Commander will immediately notify the appropriate incident commander to assemble the Management Incident Response Team (MIRT).

2.1.3. Conducting Investigations

Every Irregularity reported according to this policy will be investigated and dealt with appropriately, as determined by PHC.

In circumstances where unionized personnel are the subject of an investigation, that investigation will be conducted in compliance with any applicable Collective Agreement(s).

In circumstances where Medical Staff are the subject of an investigation, that investigation will be conducted in alignment with Medical Staff Rules. In circumstances where a Researcher is the subject of an investigation, that investigation will be conducted in alignment with any and all policies that are relevant to their affiliation.

NOTE: If the Individual under investigation has specific duties and responsibilities set out in this policy, then those duties and responsibilities will become the responsibility of their leader. For example, if the Chief Financial Officer is subject to investigation, then their duties and responsibilities will become the responsibility of the Chief Executive Officer.

All investigations will be conducted in a manner that, subject to applicable law and to the greatest extent possible, respects the individual privacy and confidentiality of everyone involved. Information will be requested and shared on a strictly need-to-know basis, to determine the validity of allegations and/or extent of Irregularities/potential Fraud.

If the Theft, Fraudulent, Corruption, and/or Extortion activity impacts the personal information of an Individual, the Information Access & Privacy Office (IAPO) will be engaged to support the investigation. If a privacy breach is confirmed, the IAPO will manage the breach in a manner consistent with the Managing Privacy Breaches Policy.

2.1.4. Responding and Resolving the Investigation

Where the investigation of an Irregularity substantiates that a PHC employee(s) has committed an act of Theft, Fraud, Corruption and/or Extortion, the HR partner,

[1] In the case of Medical Staff, the Leader is the Department or Division Head

Leadership/Management (and, where appropriate, Professional Practice) will determine:

1. The appropriate disciplinary and/or administrative measures to be applied to any employee(s) who is responsible for or has contributed to an incident of Theft, Fraud, Corruption and/or Extortion;
2. Whether the findings of the investigation should or must be reported to an external agency (e.g., law enforcement, auditor, etc.) or to a professional regulatory body; and
3. Whether further review and/or revision of existing internal controls is required to prevent future similar occurrences.

The specific action taken in any other substantiated case will be agreed by the investigative team and others as necessary, and will depend on the nature and gravity of the issue. In the case of Medical Staff this agreement may involve the Medical Advisory Committee (MAC).

For confirmed Cyber Attacks and if the attacker is identified as an external or unknown persons, the ISL Team will request support from Integrated Protection Services (IPS) and/or In-House Counsel to file a local police report. A final decision to dispose of the issue will be handled by the MIRT in consultation with the SLT or legal consultant as appropriate.

As it relates to PHC finances, with the exception of items covered under the Safe Keeping of Patient & Resident Valuables policy, pre-approval of the Chief Financial Officer (CFO) is required for any restitution arrangement or settlement with any Individual(s) as a result of findings made pursuant to an investigation under this policy.

A confidential copy of all investigation findings will be securely retained by the appointed investigator for at least two years after any decision is made about any Individual(s) in relation to the findings. Prior to destroying an investigation file, the appointed investigator will make appropriate inquiries to determine whether a longer retention period will apply.

2.1.5. Regular Reporting of Substantiated Irregularities

The Chief Financial Officer will collect and consolidate reports on substantiated Irregularities of any kind.

All substantiated financial Irregularities must be reported to the Chief Executive Officer (CEO), Chair of the Board of Directors and the Chair of the Audit and Finance Committee.

All substantiated non-financial Irregularities must be reported to the CEO, the Chair of the Board of Directors, and the Chair of the HR & Governance Committee.

The CFO will also send summary reports to applicable Board sub-committees and Internal Audit Office on a quarterly basis and to the entire Board on an annual basis. These reports will include only the following information:

- Number of Irregularities;
- Type of Irregularity (business risk); and
- The nature of process or resolution (e.g., informal resolution, mutual resolution, investigation).

2.2 Fraud Risk Management Framework

The Fraud Risk Management framework incorporates Fraud awareness, internal controls for detection and prevention of Fraud and misconduct, and ongoing monitoring of that framework to assess its effectiveness.

The CFO will send updates on the Fraud Risk Management framework to the Board and designated sub-committees on a quarterly basis.

3. Responsibilities

- **Individuals**

  All Individuals associated with PHC are responsible for complying with this policy.

- **Leadership/Management**

  Leadership/Management are responsible for communicating this policy to all of their employees and any external contractors; promoting general Fraud awareness; assuring Individual(s) comply with this policy; and implementing any corrective actions or mitigations identified as part of an investigation.

- **HR partners (People/Human Resources)**

  The HR partner is responsible for leading investigation(s) and providing support to Leadership/Management and contracted consultants during and after the investigation of any Irregularity as it relates to the employment relationship.

- **Chief Financial Officer (CFO)**

  The Chief Financial Officer (CFO) is responsible for overseeing the overall management, reporting process of irregularities and effectiveness of this policy. [The CFO is also responsible for developing and monitoring the FRM framework.]

- **Chief Information Officer (CIO)**

  For Cybercrimes, the Chief Information Officer (CIO), under PHSA, is responsible for acting as the designated Incident Commander and invoking the Management Incident Response team (MIRT) as required.

- **Chief Executive Officer (CEO)**

  The Chief Executive Officer (CEO) is responsible for escalating severe Irregularities to the Board committees and/or Board Chair as required and reviewing impact to PHC. For Cybercrimes, the CEO may also act as a designated Incident Commander to invoke the Management Incident Response team (MIRT) if required.

- **Integrated Protection Services (IPS)**

Integrated Protection Services (IPS), a lower mainland consolidated service under PHSA, is responsible for consulting and/or supporting and/or investigating any Irregularities as they relates to the physical risks to building, space, assets, or Individuals. Additionally, the IPS will act as PHC's liaison with law enforcement agencies as required.

- **Risk Management**

  Risk Management (RM) is responsible for supporting the HR partner or the appointed investigator and will liaise with the appointed investigator and with the Health Care Protection Program as and when appropriate, to determine whether a loss suffered by PHC may be insured.

- **In-House Counsel**

  In-House Counsel is responsible for providing or arranging any necessary legal support to the organization (including where necessary and appropriate for the purpose of conducting an investigation). As required, In-House Counsel will provide support to coordinate with other applicable departments that identifies potential Irregularities, current internal controls, potential gaps in current internal controls and possible mitigation strategies. Counsel may refer the investigator to external legal services as appropriate for Irregularities that require specific consultation on legislation including, but not limited to the Criminal Code.

- **Board of Directors of PHC**

  The Board of Directors is responsible for the continuous efforts of mitigation strategies; and review and evaluate exceptions to this policy in collaboration with the CEO.

  The Board Chair, the Chair of the Audit and Finance committee and the Chair of the HR and Governance committee, will ensure that the Board/committee members are briefed as appropriate on any Irregularities reported to them. They will also lead any Board/committee review of mitigation strategies put in place by PHC leadership/management as necessary.

- **Internal Audit Office (IAO)**

  Internal Audit Office (IAO) is an independent division within PHC, insofar as it reports functionally to the Board Chair through the Board's Finance and Audit Committee. Internal Audit is responsible for conducting investigations in accordance with the Board approved Internal Audit Charter. In addition to investigating Irregularities that will be identified in the ordinary course of performing assurance services, Internal Audit has the ability to investigate reported Irregularities without engaging the normal lines of management authority.

- **Communications**

  Will provide any applicable supports of incoming or outgoing information to the public and/or the investigation as required.

- **Incident Commander**

  For Cybercrimes, the designated Incident Commander (PHC's CEO or PHSA's CIO) is responsible for invoking the Management Incident Response Team (MIRT), assigning and keeping a record of assigned roles as listed in cyber Extortion playbook.

- **Information Security Leadership (ISL)**

  For Cybercrimes, Information Security Leadership (ISL), a lower mainland consolidated services at PHSA, is responsible for:

  - Maintaining, supporting and annually reviewing a Cyber Incident Response Management Plan;
  - Immediately informing, appropriate the executive leadership, CEO, In-House Counsel, and Privacy upon receipt of any Ransom or Extortion demand(s) associated with a Cyber Attack; and
  - Creating, maintaining, and increasing PHC awareness of Information Security policies and Cybercrime events noted in this Policy.

- **Management Incident Response Team (MIRT)**

  For Cybercrimes, the Management Incident Team (MIRT) is responsible for analyzing the overall risk and impact of incident and recommending a course of action to the Board.

- **Senior Leadership Team**

  For Cybercrimes, the senior leaders including Vice Presidents and CEO are responsible for analyzing the overall risk and impact of incident and recommending a course of action to the Board.

- **Biomedical Engineering Cybersecurity Project Manager**

  For Cybercrime, the Biomedical Engineering Cybersecurity Project Manager, a lower mainland consolidated service under PHC, is responsible for assessing and collaborating with the ISL team for breaches related to physical risks and/or patient systems.

4. Compliance

PHC employees who fail to comply with any provision of this policy will be subject to disciplinary action, up to and including the possibility of termination of employment.

The CFO will work with, HR partners, and Information Security Leadership to maintain effectiveness of the policy and ensure regular reporting compliance is maintained.

5. Supporting Documents

The following are related policies on the PHC Shop intranet:

- **PHC Budgets: Minor Capital Policy**
- **PHC Comfort Funds Policy**
- **PHC Conflict of Interest**
- **PHC Contract Management**
- **PHC Information Technology: Acceptable Use of Policy**
- **PHC Information Privacy and Confidentiality Policy**
- **PHC Investments**
- **PHC Managing Privacy Breaches Policy**
- **PHC Respect at Work Policy**
- **PHC Safekeeping of Patient Valuables Policy**
- **PHC Safe Reporting Policy**
- **PHC Signing Authority**
- **PHC Standard of Conduct Policy**
- **PHC Travel and Business Expense Reimbursement**
- **PHC & VCH Drug Diversion of Controlled Substances**
- **PHC Vendor Incentives and Financial Considerations**
- **PHC Working Remotely a Voluntary Basis Policy**
- **PHSA Procurement Policy**
- **VPP Information Security Policy**
- **Medical Staff Rules**

6. Definitions

Asset Misappropriation see definition of **Theft**, below.

Cybercrime is criminal activity such as Theft, Fraud and/or Extortion committed using a computer in order to illegally access, transmit, or manipulate Data. This is inclusive and not limited to ransomware, cyber Extortion, Extortion incident, Cyber Attack and cyberespionage. A crime committed with the aid of, or directly involving, a Data processing system or computer network. The computer or its Data will be the target of the crime or the computer will be the tool with which the crime is committed.

Corruption is the offering, giving, soliciting or acceptance of an improper inducement or reward for the purpose of securing an improper personal, financial or other benefit or advantage, and includes the giving and receiving of bribes.

Cyber Attack means any offensive maneuver that targets computer information systems, computer networks or infrastructures for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the Data or stealing controlled information.

Data means the following Data in the custody or control of PHC: *personal information*, as defined in privacy laws applicable to PHC; confidential information; and metadata that contains personal information, including derivative works of this Data.

Extortion means the act of using, or threatening to use, force to obtain money, services, or something else of value from a victim. In order to avoid the threatened action, an Extortion victim must pay money or perform some other actions requested by the perpetrator. The term Extortion will be used interchangeably with blackmail.

Extortion Incident means a ransomware or information Theft incident in which the attacker is demanding money from the organization to either regain control of the IT environment or to prevent the publication of sensitive Data that would result in damage to the organization or individuals involved.

Financial Statement Fraud is the intentional misrepresentation of Data in a company's financial records.

Fraud is an intentional act by one of more individuals among employees, management, those charged with governance (internal), or third parties (external) involving the use of deception/misrepresentation to obtain an unjust or illegal advantage.

Fraud Risk: risk of various types of Fraud an organization could face from internal and/or external sources

An **Individual** (and collectively defined as “Individuals”) includes:

- Members of the Board of Directors of PHC;
- All PHC employees including the Executive, management/management support and all employees on contract;
- Employees of other health organizations that serve as the agent of PHC including the participants in Lower Mainland Consolidation;
- Medical staff as defined in the PHC Medical Staff Bylaws including physicians on contract, residents and clinical trainees;
- Providers of goods and services to PHC including vendors, contractors, subcontractors and their employees;
- All researchers and members of their staff who conduct research at or under the auspices of any PHC hospitals, centres or community programs;
- Individuals authorized to access PHC’s information or systems including university faculty, support staff, students or volunteers working for or associated with PHC

Irregularity is an allegation of Theft, Fraud, and/or Corruption, including Cyber Attacks of Extortion or ransomware. An investigation of matters covered by this policy may lead to findings of Theft, Fraud, Corruption, and/or Extortion. Until a formal investigation has been conducted in accordance with this policy, all findings, reports and suspicions will be termed Irregularities.

A **Loss** is the detrimental effect or disadvantage that results from being deprived of a resource or a right to participate in an opportunity that would have otherwise legitimately benefited PHC.

Privacy Breach means the loss, Theft, intentional or inadvertent unauthorized collection, use, disclosure, storage or disposal of personal information in the custody or control of PHC.

Ransom means a sum of money demanded in exchange for something that has been taken or compromised.

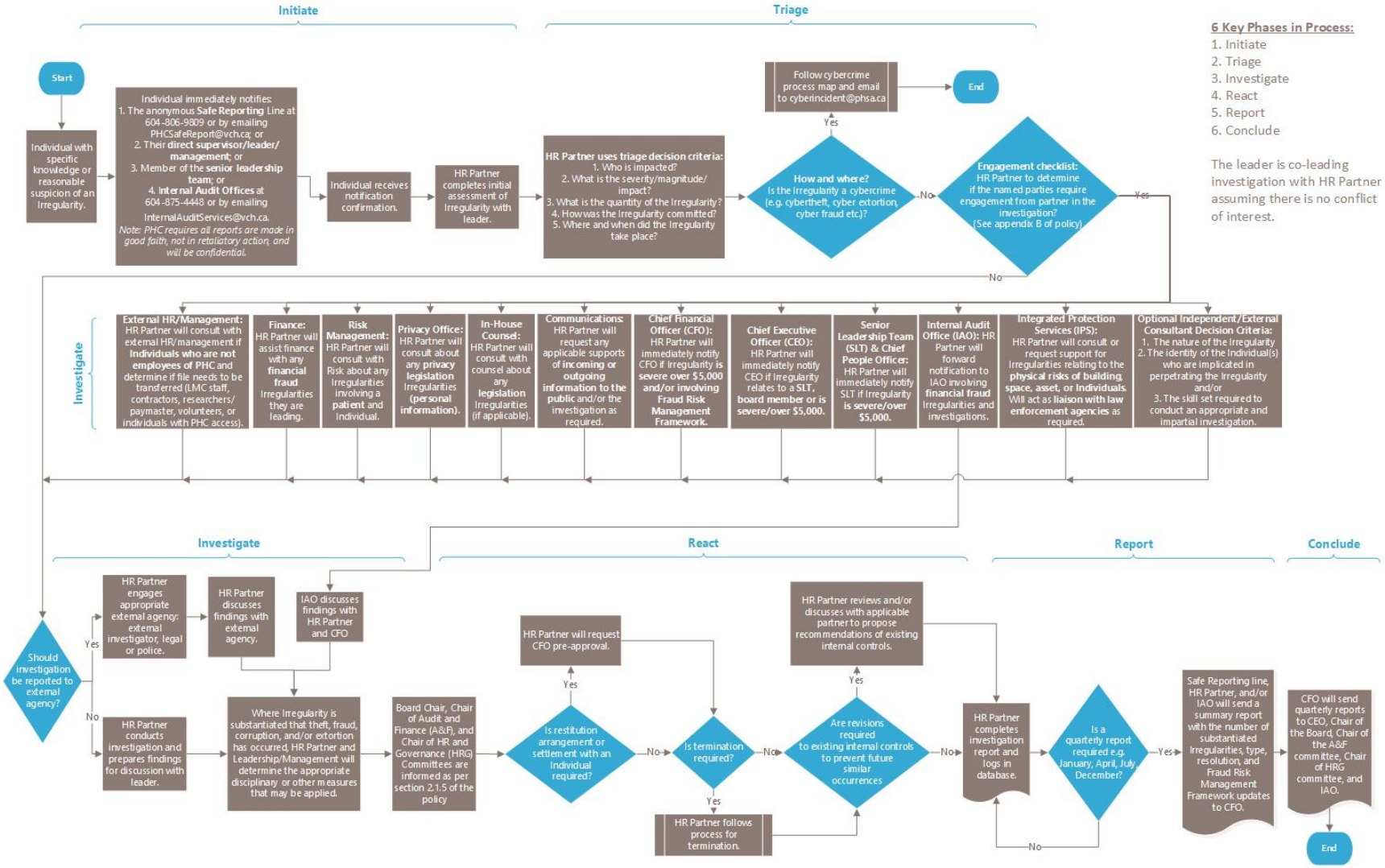
Ransomware means a type of malware that denies a user's access to a system or Data until a sum of money is paid.

Theft is a crime in which a person intentionally and fraudulently takes or removes corporate or personal property (including intellectual property, monetary or other physical goods) without permission or consent.

7. Appendices

- Appendix A: Non-Cybercrime Map
- Appendix B: Scenario and Engagement Checklist
- Appendix C: List of Contacts

Appendix A: Process Map (Non-Cybercrime Irregularities)



Appendix B: Scenarios and Engagement Checklist

Type	Scenarios (Method & Motive)	Dollar Value	HR Partner	Finance	Risk Management	Privacy	In-House Counsel	Communications	Biomedical Engineering	Chief Financial Officer	Chief Executive Officer	Senior Leadership Team (SLT) & Chief People Officer	The Chair of the Board	The Chair of the Audit and Finance Committee	The Chair of the HR and Governance Committee	Internal Audit Office	Information Security Leadership (IT)	Integrated Protection Services	Local police forces	Legal counsel (external)
Theft	Property theft: taking a belonging without consent (no personal information)	>$5K	Lead		✓		✓	✓		✓	✓	✓	✓		✓			✓	✓	✓
		<$5K	Lead															✓	✓	
	Property theft: taking a belonging without consent containing Personal Information	N/A	Lead		✓	✓	✓	✓		✓	✓	✓	✓		✓			✓	✓	✓
	Stealing money: taking money without consent	>$5K	Lead		✓		✓	✓		✓	✓	✓	✓	✓		✓			✓	✓	✓
		<$5K	Lead							✓									✓	✓	
	Time theft: accepting or claiming pay for hours not worked	>$5K	Lead	✓	✓		✓	✓		✓	✓	✓	✓		✓				✓	✓	✓
		<$5K	Lead																✓	✓	
	Willful destruction of PHC records	>$5K	Lead	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓				✓	✓	✓
		<$5K	Lead			✓													✓	✓	
	Theft and unauthorized sale of corporate data using computers or the internet e.g. hacking, social engineering, phishing, or malware	N/A	✓		✓	✓	✓	✓		✓	✓	✓	✓		✓		Lead	✓	✓	✓
	Theft of financial or card payment data using computers or the internet	N/A	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	Lead	✓	✓	✓
Fraud	Forgery or alteration of accounting or PHC records	>$5K	✓	Lead		✓	✓	✓		✓	✓	✓	✓	✓		✓		✓	✓	✓
		<$5K	✓	Lead		✓				✓						✓		✓	✓	
	Falsification of your own records: expense claims, hours worked, overtime, sick or special leave	>$5K	✓	Lead			✓	✓		✓	✓	✓	✓	✓		✓		✓	✓	✓
		<$5K	✓	Lead						✓						✓		✓	✓	
	Knowingly generating or paying fake invoices to obtain PHC funds	>$5K	✓	Lead			✓	✓		✓	✓	✓	✓	✓		✓		✓	✓	✓
		<$5K	✓	Lead						✓						✓		✓	✓	
	The intentional misrepresentation or concealment of or failure to report Irregularities to obtain an advantage (money, services or something of value)	>$5K	Lead	✓			✓	✓		✓	✓	✓	✓		✓	✓		✓	✓	✓
		<$5K	Lead	✓				✓		✓						✓		✓	✓	
	Identity or internet fraud: to use personal information without knowledge or consent	N/A	✓			✓	✓	✓		✓	✓	✓	✓		✓		Lead	✓	✓	✓
Corruption	Intentionally failing to follow PHC procedures or act of dishonesty in handling money or reporting financial transactions	N/A	✓	Lead			✓	✓		✓	✓	✓	✓	✓		✓		✓	✓	✓
	Unusual compensation, benefits or rights received by Individuals in exchange for actual or perceived goods, services, advantages or benefits	N/A	Lead	✓			✓	✓		✓	✓	✓	✓	✓		✓		✓	✓	✓

Type	Scenarios (Method & Motive)	Dollar Value	HR Partner	Finance	Risk Management	Privacy	In-House Counsel	Communications	Biomedical Engineering	Chief Financial Officer	Chief Executive Officer	Senior Leadership Team (SLT) & Chief People Officer	The Chair of the Board	The Chair of the Audit and Finance Committee	The Chair of the HR and Governance Committee	Internal Audit Office	Information Security Leadership (IT)	Integrated Protection Services	Local police forces	Legal counsel (external)
Extortion	Blackmail: demanding money, services or something of value from an Individual or PHC in return for not revealing compromising or damaging information about them	N/A	Lead			✓	✓	✓		✓	✓	✓	✓		✓			✓	✓	✓
	An agreement or perceived agreement between two or more persons to commit an act that knowingly circumvents internal controls	N/A	Lead	✓		✓	✓	✓		✓	✓	✓	✓		✓			✓	✓	✓
	A ransomware or information theft incident in which the attacker is demanding money, services or something of value from an Individual or PHC to prevent the publication of sensitive data that would result in damage	N/A	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓		Lead	✓	✓	✓
	A ransomware or information theft incident in which the attacker is demanding money, services or something of value from an Individual or PHC to either regain control of the IT environment that would result in damage	N/A	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	Lead	✓	✓	✓
	Intentional misuse of IT property, facilities or services including confidential information and/or intellectual property in return for an advantage (exchange for money, services, or something of value)	N/A	✓			✓	✓	✓		✓	✓	✓	✓	✓	✓		Lead	✓	✓	✓
	Threat of a cyber attack to damage/disable patient systems in exchange for an advantage (money, services, or something of value)	N/A	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		Lead	✓	✓	✓

NOTES:

1. Over $5K can also be severe incidents that should be escalated
2. Finance is the lead for all financial fraud regardless of the amount
3. Finance may records transactional losses of incidents
4. Risk Management is also involved for potential insurance claims

DEFINITIONS:

Corruption is the offering, giving, soliciting or acceptance of an improper inducement or reward for the purpose of securing an improper personal, financial or other benefit or advantage, and includes the giving and receiving of

Cybercrime is criminal activity such as Theft, Fraud and/or Extortion committed using a computer in order to illegally access, transmit, or manipulate Data. This is inclusive and not limited to ransomware, cyber Extortion, Extortion incident, Cyber Attack and cyberespionage. A crime committed with the aid of, or directly involving, a Data processing system or computer network. The computer or its Data will be the target of the crime or the computer will be the tool with which the crime is committed.

Cyber Attack: An attack that involves the unauthorized use, manipulation, interruption or destruction of, or access to, via electronic means, electronic information or the electronic devices or computer systems and networks used to process, transmit or store that information.

Extortion: Act of using, or threatening to use, force to obtain money, services, or something else of value from a victim. In order to avoid the threatened action, an extortion victim must pay money or perform some other actions requested by the perpetrator. E.g. blackmail.

Fraud is an intentional act by one of more individuals among employees, management, those charged with governance (internal), or third parties (external) involving the use of deception/misrepresentation to obtain an unjust or illeagal advantage.

Irregularity is an allegation of Theft, Fraud, and/or Corruption, including Cyber Attacks of Extortion or ransomware. An investigation of matters covered by this policy may lead to findings of Theft, Fraud, Corruption, and/or Extortion. Until a formal investigation has been conducted in accordance with this policy, all findings, reports and suspicions will be termed Irregularities.

Theft is a crime in which a person intentionally and fraudulently takes or removes corporate or personal property (including intellectual property, monetary or other physical goods) without permission or consent.

Appendix C: List of Contacts

Type of Irregularity	Report To	Contact Information
Any Theft/Fraud/Corruption irregularity except as noted below	Direct Supervisor, Leader, or Management or PHC Safe Reporting Line	Variable
Irregularity involving supervisor, or if not comfortable reporting to supervisor	PHC Safe Reporting Line	Risk Management Office 3rd floor, 1190 Hornby St, Vancouver, BC, V6Z 2K5 604-806-9809 or PHCSafeReport@vch.ca
Irregularities concerning financial records and/or monetary items	Executive Director, Internal Audit Office	Internal Audit Services M10-601 W. Broadway 604-875-4448 or Email: InternalAuditServices@vch.ca
Irregularity involving cybersecurity	PHSA Information Security Leadership	cyberincident@phsa.ca
Irregularities relating to information privacy	Information Access and Privacy Office	Information Privacy Office 11th floor, 1190 Hornby St, Vancouver, BC, V6Z 2K5 or privacy@providencehealth.bc.ca
Irregularities relating to intellectual property or involving Internal Audit Office	In-House Counsel	In-House Counsel 3rd floor, 1190 Hornby St, Vancouver, BC, V6Z 2K5 or cciarniello@providencehealth.bc.ca
Reports involving Board Members, CEO or members of Senior Leadership Team	PHC Safe Reporting Line	3rd floor, 1190 Hornby St, Vancouver, BC, V6Z 2K5 604-806-9809 or PHCSafeReport@vch.ca
Reports involving the PHC Board Chair	Minister of Health	Room 337, Parliament Buildings Victoria, BC V8V 1X4 Phone: (250) 953-3547, Fax: (250) 356-9587, or E-mail: hlth.minister@gov.bc.ca
Reports involving Criminal Law	Local police forces	Online list is available at BC's government website.
Reports involving correction of safety hazards and unsafe conditions made in accordance with the provisions of WorkSafe BC's Occupational Health and Safety Regulations	PHC Occupational Health & Safety	3rd floor, 1190 Hornby St, Vancouver, BC, V6Z 2K5 OHS@providencehealth.bc.ca

Effective Date:	16-Aug-2022			
First Released:	19-Nov-2013			
Last Revised:	16-Aug-2022			
Last Reviewed:	16-Aug-2022			
Approved By:	PHC Senior Leadership Team			
Owners:	PHC Finance			
Revision History:	**Version**	**Date**	**Description/ Key Changes**	**Revised By**
	1	19-Nov-2013	Approval of policy	Risk Management & Patient Safety, VP Human Resources and General Counsel
	2	Aug 2022	Review and revision of policy	People, Finance, Risk Management, Patient Safety, and Privacy