Strengthening digital defence: Privacy and Cyber, working in partnership.

Protecting Privacy in Cyber Incidents. A guide for the Healthcare Sector.

STOP! If you are currently experiencing a live privacy breach incident, go to **page 12** for immediate response steps.

Health New Zealand
Te Whatu Ora

Contents

Acknowledgments

This resource was developed with the support of people from across the Primary Healthcare Sector, including from Primary Health Organisations and Regulatory organisations. Their participation helped to co-design privacy advice which holds real-life experience and clinical priorities at its core.

Published 2025

1 - Introduction

This handbook is designed to help navigate the complex landscape of responding to a cyber privacy breach.

It will outline the essential steps required for an organisation to quickly recover and resume operations. From identifying and containing the breach to communicating with stakeholders and restoring systems, this handbook provides practical advice and actionable steps helping to minimise damage and regain control. This handbook is structured around a well-established risk management approach - the Four Rs Framework; Reduction, Readiness, Response, Recovery - which we have adapted for the context of cyber privacy breaches.

Equipping the organisation with the knowledge and tools necessary to respond will ensure privacy breaches and incidents are swiftly and effectively managed, ensuring your organisation can weather the storm and emerge stronger.

Whether you are a small business owner, an IT professional, or a member of your organisation's leadership team, this booklet will serve as a valuable resource in your efforts to protect your organisation's privacy and security.

Imagine:

- How would you continue **business as usual** if your **systems went down?**
- How would you get the **systems back online?**
- How would you manage your **current workload** while **responding to this crisis?**
- Who would you contact for **immediate assistance** and **guidance?**
- How will you **tell** your **staff, patients, community, stakeholders?**

Why is health information a target for cyber criminals?

Patient data vulnerability:

Health information is a prime target for cyber criminals due to its sensitive nature and market value. It is at risk as it's constantly updated and exchanged which means it is current and more valuable.

Data exchange risks:

The constant digital and physical exchange of health data among various clinicians, systems, and facilities heightens its exposure and makes it more vulnerable.

Cyber security lag:

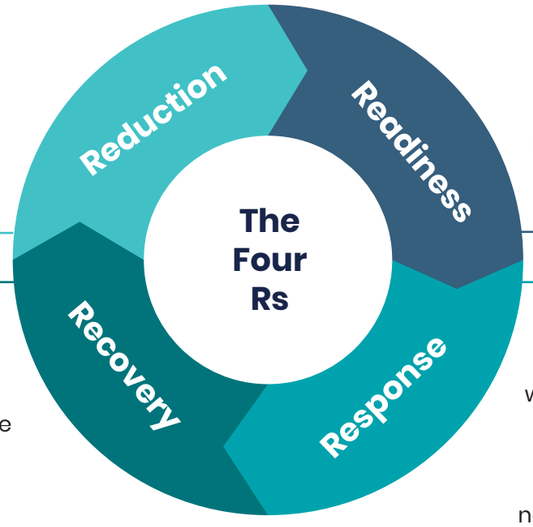
Health information systems struggle to keep pace with rapid cyber technology advancements, leaving them exposed, with cyber criminals able to exploit vulnerabilities and access sensitive health data.

2 - The Four Rs

The Four Rs framework - **Reduction, Readiness, Response, Recovery** - Is a well established emergency response framework. It serves as a comprehensive approach to managing risks, particularly useful in the context of privacy breaches and information security in healthcare settings.

Reduction

Implement measures to **decrease** the likelihood and impact of potential breaches. This includes **strengthening** security protocols, performing regular risk assessments, and educating stakeholders on best practices.



Readiness

Ensure that systems and teams are **prepared** to handle potential breaches. This involves creating and updating incident response plans, training staff, and conducting regular drills to **simulate breach scenarios**.

Recovery

Focus on **restoring** normal operations and addressing any damage caused by the breach. Consider all aspects of the incident to **improve future** breach response efforts.

Response

Take **immediate action** when a breach occurs to **mitigate** its effects. This includes identifying and containing the breach, notifying affected parties, and implementing measures to **prevent further damage.**

2.1 - Reduction

Implement measures to decrease the likelihood and impact of potential breaches. This includes strengthening security protocols, performing regular risk assessments, and educating stakeholders on best practices.

What are some of the risks to organisations when collecting, using, and holding health information?

Compliance risks

- Failure to comply with the Privacy Act 2020 and the Health Information Privacy Code 2020.
- Unclear policies and procedures for data storage, security, access, correction, retention, disposal, and disclosure.

Technological risks

- Vulnerabilities in IT systems and software that could be exploited by cyber criminals.
- Risks associated with the storage and transmission of personal information digitally; including hacking, malware, and phishing attacks.

Human-related risks

- Errors or negligence by staff members leading to unauthorised access to, or disclosure of, personal information.
- Insider threats, where employees deliberately misuse or steal personal information.

Take a moment to consider and note down the immediate risks you identify in relation to your business/organisation and verify they are included in your risk management procedures for tracking.

Risks organisations encounter in relation to privacy breaches:

Operational risks

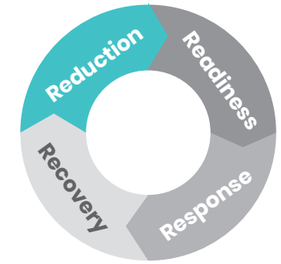
- Disruption to day-to-day operations in the event of a privacy breach.
- Resource allocation to manage and mitigate breaches, which can divert attention away from primary healthcare services.

Reputational risks

- Damage to the organisation's reputation and loss of trust among patients and the community.
- Negative media coverage that can impact the organisation's relationships with stakeholders.

Financial risks

- Costs associated with support e.g. IT, legal, and potential fines.
- Potential compensation to individuals whose privacy has been compromised.

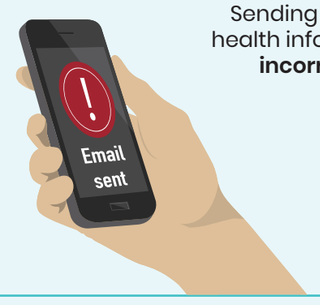


Understanding privacy breaches. What are your individual privacy risks?

A privacy breach occurs when personal information held by an organisation is accessed, disclosed, altered, lost, or destroyed without proper authorisation (either intentionally or unintentionally).

Examples of breaches include:

Improper disposal of rubbish containing personal information



Sending a letter, email, health information to an **incorrect individual**

Being a victim of theft and having a laptop or documents containing health information **stolen**

Clicking a **phishing link** which results in a cyber attack

What is a notifiable privacy breach?

Under s 112 of the Privacy Act 2020, a notifiable privacy breach is one that has either caused, or is likely to cause, **serious harm to someone whose information was impacted by the breach.**

Every privacy breach should be assessed on a case-by-case basis.

As per the Privacy Act 2020, s 112 - organisations **must** notify the Office of the Privacy Commissioner (OPC) as soon as practicable after becoming aware that a notifiable privacy breach has occurred.

It is expected that notification should occur within **72 hours** of identifying the breach.

The online OPC tool **NotifyUs** is available to help determine if a breach is significant enough to warrant notification.

2.1 - Reduction

Good practice to reduce the likelihood of a privacy breach includes:

1. Improving privacy awareness and training

- **Understand and follow privacy laws:** Ensure staff compliance with the Privacy Act 2020 and Health Information Privacy Code 2020. Stay updated on legislative changes and keep staff informed of their responsibilities.
- **Learn from each other:** Conduct interactive sessions for team members to share privacy experiences, learnings, and voice concerns in an open environment.

2. Strengthening technology safeguards

- **Boost cyber security:** Fix weaknesses in your computer systems to protect against threats like hacking or phishing. Make sure your cyber security measures are strong and up-to-date.
- **Employ strong passwords:** Enable a culture of secure password users. See **The Cyber Hub - Creating Strong Passwords** for more guidance.
- **Use multi-factor authentication (MFA):** Add an extra layer of security by requiring more than one method of verification to access user accounts.
- **Conduct privacy impact assessment (PIA):** Use a PIA to identify and mitigate privacy risks when starting new projects or changing how personal information is handled. See **The Cyber Hub - Privacy Impact Assessment (PIA)** for more guidance.

3. Understanding personal and health information

- **Educate the team:** so that everyone is familiar with the definition of personal and health information. Personal Information consists of data that can directly (like a name) or indirectly (like an address) identify a person. More data points increase the ease of identification. Health Information includes details about an individual's health services. It covers medical history, health conditions and health or disability service records.

4. Managing vendors and contracts

- **Verify contracts with vendors are up-to-date:** Make sure vendor contracts, especially IT systems and insurance, are reviewed yearly or after any cyber attacks or breaches to verify all relevant required updates are included.
- **Verify your coverage:** Determine whether your IT provider will assist in all types of cyber attacks. Verify what your insurance covers, and what assistance they will provide.

Key Tip:

Stay informed!

Keep your eyes peeled for what is going on nationally and internationally. This is the best way to stay ahead. Stay aware of changes in legislation and act accordingly.

5. Reduce potential for human errors

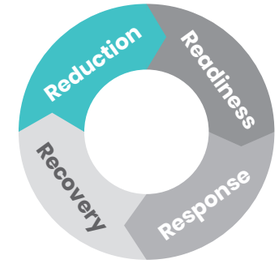
- **Share information safely:** Investigate and select a secure platform for distributing files containing personal or health information, such as those shared between healthcare providers and patients.
- **Email best practices:** Verify email recipients and use 'bcc' for group messages to safeguard privacy. Also, carefully select and send only essential attachments.

6. Provide clear guidance

- **Establish policies and procedures**: Implement clear policies and procedures for handling and protecting information. It is helpful to base these off the Information Privacy Principles in the Privacy Act 2020.

7. Conduct risk assessments

- **Identify vulnerabilities:** Regularly evaluate risks to pinpoint and mitigate system vulnerabilities, potentially in collaboration with your IT provider.
- **Prioritise risks:** Identify and rank risks based on criticality of assets and the sensitivity of the information they contain to prioritise effectively.



Key Tip:

Pause before you click send to check recipients and remember, don't click on links unless they are from a source you trust and hover the pointer over the link to verify it is sending you to the site you expect.

How a systematic reduction process helped

Example:

A healthcare clinic conducted a routine risk assessment as part of their ongoing efforts to enhance information security.

During the assessment, identified vulnerabilities in their Patient Management System (PMS) that could potentially have exposed patient information.

An example of how a routine assessment helped identify vulnerabilities:

- **Risk assessment:** The clinic proactively identified vulnerabilities in their PMS through a comprehensive risk assessment process. They prioritised these vulnerabilities and coordinated with their IT provider for immediate patches and updates.
- **Training and learning:** The clinic conducts training sessions for staff members around the importance of safeguarding patient information, recognising phishing attempts, and handling patient records securely with MFA access enabled. Interactive sessions are regularly held discussing team members' privacy experiences.
- **Policy development**: The clinic has clear policies and procedures aligning to the principles in the Privacy Act 2020 and Health Information Privacy Code 2020. As part of their security policy, they review their vendor contracts regularly.

2.2 - Readiness

Please see **Strengthen Your Digital Defence - A Guide to Cyber Security Incident Response for New Zealand Primary Health Sector** for further information on roles and responsibilities. As an organisation, there are several readiness steps that can be undertaken to respond quickly and reduce damage. These include:

1. Exercises and scenarios:

- **Conduct exercises:** Plan regular exercises to practice responding to different scales of privacy breaches or incidents. Keep these current, relevant, and engaging so staff are continuously learning.
  - For **staff:** Teach them to recognise signs of a privacy breach and the immediate actions to take when they occur.
  - For **incident response team (IRT) members:** Train them in their IRT roles and conduct regular scenarios so they know what's expected of them and feel comfortable in their roles.
- **Develop contingency:** Rotate staff around roles in exercises or scenarios to help build confidence and competence.
- **Seek feedback:** Ask staff for their feedback - this is a great way to identify gaps in knowledge and can help plan further scenarios.
- **Support and encourage:** Enable staff to ask questions or highlight cyber security and privacy concerns.

2. Monitor and detect:

- **Continuous monitoring:** Understand what your external/in-house IT provider will be monitoring and discuss with them what you need to keep an eye on.
- **Detection:** Gain an understanding of how to detect a potential breach and how an alert may be shared.
- **Audit and access:** Verify that IT (responsible) and senior clinical staff (accountable) are working together to enforce user access controls, audit the appropriateness of access, and maintain logs and audit trails to monitor activity and support investigations into any breaches or incidents.

Key Tip:

Cyber security and privacy begin at an individual level.

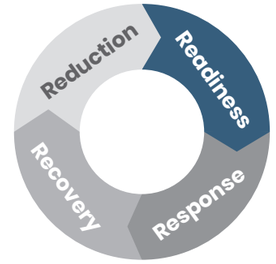
Consider educating staff on their personal security and privacy practices, this will heighten awareness and benefit the workplace.

Call Tree:

Make sure your call tree is up to date.
See Call Tree Page 21.

Key Tip:

Socialise clear policies across teams so staff members know what they should and shouldn't be accessing.



When readiness helped

Example:

A small healthcare business recently became a target of a sophisticated cyber attack through a phishing email campaign. A staff member clicked on a link enabling attackers to infiltrate the network – the staff member promptly told the practice manager.

Within the next hour the IT provider identified that patient information had been taken.

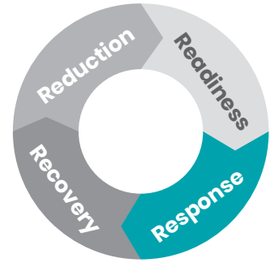
An example of a breach, how it played out, and how being ready helped the organisation limit the impact of the attack:

- **Incident response plan:** The team swiftly activated the pre-established incident response plan (developed following the **Strengthen Your Digital Defence - A Guide to Cyber Security Incident Response for New Zealand Primary Health Sector**), which includes specific protocols for breach detection, containment, investigation, and notification.
- **Drills and simulations:** Regular drills and simulations trained staff to recognise and report suspicious links to their IT provider, preventing further compromise.
- **Monitoring:** The IT provider quickly detected unauthorised access, isolated the affected systems, and limited the impact of the breach.

- **Privacy breach response plan:** The team swiftly activated the pre-established privacy breach response plan to help manage the privacy breach.
- **Communication plan:** Using prepared communication templates, the business promptly notified their internal staff. The IRT used templates to start drafting external communications to patients, regulatory authorities, and stakeholders. This transparent communication helped maintain trust and compliance with legal obligations.

2.3 Response - Immediate Response Steps

Use this step-by-step guide to respond to a privacy breach incident. For more details, refer to OPC's principles and website tool NotifyUs to get more support. This response process can be used as a pull out for ease of reference in an active incident.



Incident Detected

Contain the privacy breach

Contain

Immediately contain a privacy breach by:

- **Recovering** lost information.
- **Disabling** affected systems.
- **Containing information.**

Activate (IRT) or If you don't have a response team, assign competent individuals to conduct a preliminary investigation.

Consider contacting internal and external experts for **support**:

- IT providers.
- Insurer.
- Primary Healthcare Organisation (PHO).
- Legal advisor.
- External agencies: National Cyber Security Centre (NCSC), NetSafe, Police.

Assess

Assess the impact and severity of the incident

Identify the **cause of the breach.**

Identify the extent of the breach:

- How many people affected?
- How many recipients of the information?
- Who are the recipients? E.g; Malicious actors?

Identify the **potential harm to INDIVIDUALS** resulting from the breach:

- Identity theft.
- Financial loss.
- Loss of business or employment opportunities.
- Significant humiliation or loss of dignity.

Identify the sensitivity of the personal information.

Did the **Contain** actions mitigate the risk of harm?

If you have a response plan, follow your severity assessment. Otherwise, refer to the OPC website tool NotifyUs to assist your assessment.

If you have cyber incident insurance and legal counsel, engage your provider(s) early.

Notify Police if the breach appears to involve theft or other criminal activity.

Examples of extreme harm can include:

- Imminent threats to national security.
- Physical violence or kidnapping.
- Financial hardship.
- Risk to someone's life.

Please refer to **page 21 for a "Call Tree"** detailing a full list of people you may want to consider notifying a privacy breach.

You need to notify the Office of the Privacy Commissioner (OPC) within 72 hours if you believe you have had a data or privacy breach that could cause serious harm.

Notify all the relevant parties

To ensure you comply with notification requirements - review Part 6 of the Privacy Act 2020 some examples of things you will need to include in your notification are:

- Details of the incident.
- Description of compromised data.
- Affected individuals.
- Actions taken to safeguard the data.
- Support measures for individuals.
- Notification to the OPC.
- Contact details for further information.
- The Individual's right to complain to the OPC.

Consider confidentiality obligations and decide on notifying relevant third parties to get more support, such as NCSC and NetSafe.

Notify

Prevent

Prevent future breaches

Conduct detailed **Lessons Learned with all stakeholders involved in the response** to identify and address gaps:

- **Ask** - what went well? What didn't go well?
- **Ask** - how can the organisation reduce the likelihood of a data breach occurring?

Stakeholder Management:

- Maintain **open and transparent communication** with internal and external stakeholders throughout the recovery process.

Business Continuity Plan (BCP):

- What practices need to be enhanced?

Risk Management and Mitigation:

- **Business Operations:** Gradually bring business operations back to normal under enhanced scrutiny. This may involve temporary measures or adjustments to normal operations while certain systems are under review.
- **Staff Training:** Use the incident as a training opportunity. Encourage staff to feedback on their experiences.
- **Post Breach Review:** Conduct a detailed review to understand the root causes of the breach, the effectiveness of the response, and to identify areas that need to be improved or changes required to policies and procedures.
- **Policies and Procedures:** Review and update policies and procedures to reflect amended or additional requirements required following guidance provided in this handbook.

Incident Closed

2.3 - Response

The Office of the Privacy Commissioner (OPC) comprehensive steps

The OPC provides comprehensive steps for managing privacy breaches, focusing on four key actions: **Contain, Assess, Notify and Prevent.** Take **immediate action** when a breach occurs to mitigate its effects.

Contain	Assess	Notify	Prevent
Immediately take steps as outlined on the following page 12 to stop the breach and secure the impacted information. This minimises further exposure and mitigates potential harm.	Evaluate the breach to understand the scope and impact. This is where you determine what information was involved, how it was compromised and the potential risks to any individuals.	Tell the individuals whose information was impacted, as well as relevant authorities and stakeholders. Timely notification allows impacted individuals to protect themselves and access support as required.	Implement measures to prevent future breaches. This includes reviewing and improving security protocols, staff training, and ensuring ongoing monitoring in information protection practices.

This is our interpretation of the Contain, Assess, Notify, Prevent framework.

Please refer to the OPC website or the Privacy Act 2020 for more information.
https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/

How to evaluate the severity of a privacy breach

Consider the following factors to evaluate the severity of a privacy breach. However, each breach should be considered on its own merits.

What is serious harm?

In New Zealand, "serious harm" from a privacy breach refers to significant negative effects that may arise from unauthorised or accidental sharing, exposure, use, or loss of personal information that can seriously harm **individuals or groups.**

Certain information is more sensitive than others and may be more likely to cause harm. In addition, some individuals may be more vulnerable than others.

Serious harm can manifest as:

- Identity theft.
- Financial loss.
- Reputational damage.
- Emotional distress.
- Physical harm.

Section 113 of the Privacy Act 2020 outlines the assessment of the likelihood of serious harm being caused by a privacy breach.

Remember – every breach is different and must be considered on its individual characteristics.

Office of the Privacy Commissioners – NotifyUs Tool

The OPC NotifyUs tool is a self-assessment guide to help you understand whether you need to notify the breach to the OPC.

This is a guide and is not exhaustive. There may be other relevant factors to consider in your serious harm assessment.

Please refer to the OPC website or the Privacy Act 2020 for more information.
https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/

2.3 - Response

Factors influencing serious harm

When assessing whether your privacy breach is likely to cause serious harm (and therefore become a notifiable privacy breach), the following factors should be considered, as set out in s.113 of the Privacy Act:

1

Sensitivity of information

The more sensitive the information (like health or financial data), the greater the potential for serious harm if disclosed.

2

Mitigation actions

Steps you have taken to reduce the risk of serious harm, such as recovering the lost information or wiping a stolen device remotely.

3

Security measures

Strong security measures like encryption and password protection help reduce the risk of data being misused if a breach occurs.

4

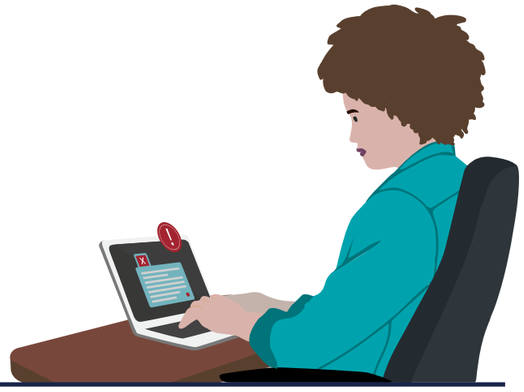
The Recipients

The risk of harm increases if data falls into the hands of those with malicious intent or unknown third parties who might misuse it.

5

Nature of harm

What is the nature of harm that may be caused to impacted individuals e.g. emotional, financial, reputational, physical.



This is a guide and is not exhaustive. There may be other relevant factors to consider in your serious harm assessment.

Please refer to the OPC website or the Privacy Act 2020 for more information.
https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/

2.4 - Recovery

Undertaking a comprehensive lessons learned is a vital part of the recovery process

This limits damage to your business, reduces your future risk, and improves your response capabilities. Focus on restoring normal operations and addressing any damage caused by the breach. Consider all aspects of the incident to improve future breach response efforts.

Business operations: Gradually bring business operations back to normal under enhanced scrutiny. This may involve temporary measures or adjustments to normal operations while certain systems are under review.

Staff training: Use the incident as a training opportunity. Encourage staff to feedback on their experiences.

Post breach review: Conduct a detailed review to understand the root causes of the breach, the effectiveness of the response, and to identify areas that need to be improved or changes required to policies and procedures.

Policies and procedures: Review and update policies and procedures to reflect amended or additional requirements required following guidance provided in this handbook.

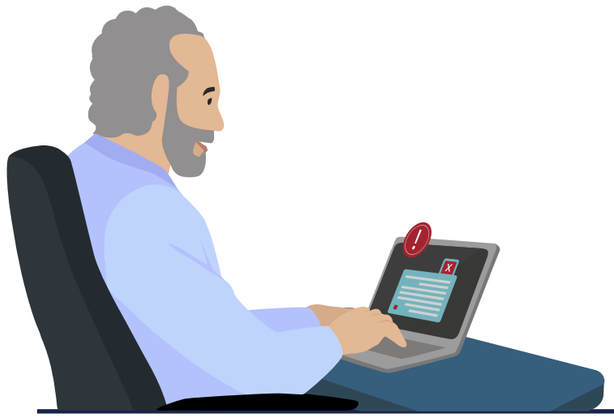
Regulatory reporting: Complete any required follow-up reporting with regulatory bodies, detailing the breach impacts and the corrective actions taken.

Restore data and systems: Use secure backups to restore lost or compromised data and systems. Verify that all restored systems are free from malware and vulnerabilities.

Restore trust: With all stakeholders including patients, staff and community. Provide regular updates about remedial actions and security enhancements to regain confidence.

Security improvement: Implement security improvements based on findings from the post-breach analysis, such as updating software and managing vulnerabilities.

Continuous improvement: Consider enhancing monitoring tools driven by regular assessments and feedback loops.



How a systematic recovery process helped

Example:

A medium-sized healthcare provider experienced a data breach involving patient records due to a cyber attack on their PMS.

The breach compromised sensitive health information, including patient diagnoses, treatment histories, and personal identifiers.

Once they worked through the immediate response (they contained, assessed, notified, and prevented), they then turned to recovery.

An example of how following a breach an organisation rebuilt systems and trust, and hardened their processes and technology:

Technology restoration

- Patient records were restored from encrypted backups to enable continuity of care.
- Security vulnerabilities were addressed to enhance PMS protection. Additional security measures, such as enhanced access controls and encryption protocols, were implemented to prevent future incidents.

Post breach review and compliance

- A detailed post-breach analysis was conducted to improve incident response and cyber security policies based on lessons learned.

Restore trust and regulatory reporting

- The healthcare provider prioritised transparent communication with the regulator and stakeholders. Throughout the recovery process, the healthcare provider prioritised patient care continuity with measures to minimise disruptions to medical services and reassured patients of their commitment to safeguarding patient information and privacy.

Staff training

- The healthcare provider used this incident as a training opportunity. They incorporated staff feedback into their post breach review and developed similar training scenarios to prevent future incidents.

Key Tip:

If you have cyber incident insurance and legal counsel engage your provider(s) early in the response as they can help you respond effectively.

3 – Useful Resources

Reporting a cyber security Incident

If you do experience a cyber security incident, you may need to notify various New Zealand Government agencies:

- Under the Privacy Act 2020, if you have a confirmed or suspected a data breach and the threshold of serious harm is met, you should **report this to the OPC** within 72 hours. The OPC also offers **FREE online training** regarding your responsibilities in a privacy breach.
- Cyber security incidents can be reported to CERT NZ. They will help you to identify the type of incident and what some next steps should be. They may also refer you to other partner agencies, with your permission. Reporting details can be found on **CERT NZ website.**
- NZ Police – if you believe a crime has been committed, report it to NZ Police by calling 105 (for non-emergencies).

Cyber Hub

The Cyber Hub: (https://www.tewhatuora.govt.nz/health-services-and-programmes/cyber-hub) provides information and advice to the New Zealand health sector about cyber security, including tools and templates. Health New Zealand will continue update the Cyber Hub with material regularly, so check it out whenever you can!

Further reading

These resources provide additional advice on best practice in privacy and support around cyber security:

- **Office of the Privacy Commissioner:** https://www.privacy.org.nz/
- **OPC – privacy online training courses -** free online learning modules on a range of privacy-related topics.
- **OPC – privacy breach guidelines –** provide detailed guidance on how to prevent and respond privacy breach.
- **OPC – notification content –** provide detailed guidance about what content should be included in a notifiable privacy breach.
- **OPC - PIA toolkit** – a systematic approach organisations to evaluate and mitigate privacy risks associated with personal data.
- For further information and a link to the **Health Information Security Framework (HISF)**, the link can be found here Health Information Security Framework.
- **HISF** has put together guidance documentation designed to support micro to small organisations and practitioners holding patient personally identifiable health information.
- **CERT NZ** data breaches– a useful guidance for business handling data breach.
- **CERT NZ** cyber security for staff – top tips on how you can educate your staff to be aware of cyber security risk and best practice.
- **CERT NZ** compiles an annual list of the most critical controls that if implemented correctly would prevent, detect, or contain the majority of the attacks seen in NZ in the last year.
- **Digital:** https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-organisations/

4.1 - Rapid Risk Assessment

A rapid risk assessment in the context of a privacy breach is a crucial initial step immediately after discovering a breach. It's aimed at quickly evaluating the scope, impact, and potential consequences of the breach to guide immediate response actions. This assessment helps determine the severity of the breach and informs decisions on containment, notification, and mitigation strategies.

Purpose of a Rapid Risk Assessment

- **Identify the Nature of the Breach:** Understanding what type of data has been compromised (e.g., health information, personal or sensitive) and how the breach occurred (e.g., hacking, physical theft, insider threat).
- **Scope and Scale:** Determining how much data is affected and how many individuals are potentially impacted.
- **Assess Immediate Threats:** Evaluating if ongoing data loss is happening and needs immediate stopping.
- **Legal and Compliance Implication Rapid Assessment:** Identifying any legal obligations for reporting the breach to regulatory authorities and affected individuals.
- **Risk of Harm:** Difficult to ascertain but could be gauged by type of loss (major clinical system with full access), by whom has accessed the data (insider, trusted person accidental access, likely overseas actor).

Steps in Conducting a Rapid Risk Assessment

Gather Information:

- Collect all relevant information about the breach, including when, how, and what data was affected.
- Determine the systems, locations, and parties involved.

Evaluate the Impact:

- Assess the sensitivity of the compromised data and the impact on affected individuals (e.g., risk of identity theft, loss of highly sensitive health information).
- Consider the implications for the organisation, such as reputational damage, regulatory penalties, or financial costs.

Determine the Likelihood of Further Harm:

- Analyse the potential for additional data loss or further unauthorised access.
- Evaluate the effectiveness of the current containment measures.

Prioritise Actions Based on Risk:

- Identify critical actions needed to contain the breach.
- Prioritise notifications based on the severity and potential harm to individuals and compliance requirements.

Document and Communicate:

- Record the findings of the risk assessment.
- Communicate the results to key decision-makers to coordinate the response.

Tools and Considerations

Incident Response Team: Utilise a dedicated team that can mobilise quickly to conduct the assessment and begin containment.

Checklists and Pre-Defined Criteria: Develop and use checklists or criteria to streamline the assessment process. These tools help ensure no critical element is overlooked during the hectic initial response phase.

Continuous Monitoring: Keep assessing and updating the risk evaluation as new information becomes available or as the situation evolves.

A rapid risk assessment is dynamic and should be adjusted as the situation develops. Its primary goal is to quickly provide a clear understanding of the breach to facilitate an effective and proportionate response, minimising harm and restoring trust and security.

4.2 - Call Tree

When experiencing a privacy breach it is good to have in your plans who you may need to contact.

All privacy breaches should be treated on a case-by-case basis and not all these contacts may be required or applicable to your breach:

- **Team Leader:** to co-ordinate and lead the response team.
- **Privacy Officer:** to bring privacy expertise to the team.
- **Legal Support:** to identify legal obligations and provide advice.
- **IT Support:** this role can help establish the cause and impact of a data breach that involved IT systems.
- **PHO:** to provide support and offer past-privacy breach experience.
- **Insurance Provider:** to manage the response process and assist with liability.
- **Human Resources (HR) support:** to provide support to staff.
- **Media/Communications Expertise:** to assist in communicating with affected individuals and dealing with the media and external stakeholders.

Prepare a contact list with internal and external stakeholders to help you rapidly respond the privacy breach.

OPC
Phone: 0800 803 909
Email: enquiries@privacy.org.nz

4.3 - Glossary

Terms	Definition
Asset	Any piece of information, software or hardware that an organisation uses in the course of its business activities.
Antivirus software	A specific software used to prevent, scan, detect and delete viruses from a computer.
Backup	A copy of a file or other item of data made in case the original is lost or damaged.
Business Continuity Plan (BCP)	A BCP includes documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.
CERT NZ	New Zealand Government agency that supports businesses, organisations and individuals affected by cyber security incidents and provides trusted advice.
Cyber security hygiene	Cyber security hygiene refers to fundamental cyber security best practices that an organisation can undertake. Cyber hygiene best practices help protect the health of your organisation's network and assets.
Cyber security incident	A cyber security incident is a breach of the security rules that puts – or has the potential to put – your information or the systems you use at risk.
Data	Data is a type of information (especially facts or numbers) that is collected to be categorised, analysed, and/or used to help decision making.
DDoS	DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cyber crime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.
Disaster Recovery Plan	A disaster recovery plan is written in partnership with your IT provider and contains instructions on how to rebuild specific essential systems and IT infrastructure, including back ups of important data.
Endpoint Detection and response (EDR)	A solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.
Firewall	A barrier that sits between a private internal network and the public internet.
Identity Theft	Identity theft is the deliberate use of someone else's identifying information, typically as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss.
Incident Response	The effort to quickly identify an attack, reduce its effects, contain damage and remediate the cause to reduce risk of future incidents.
Incident Response Team (IRT)	A dedicated team to tackle Cyber Security Incidents. The team may consist of Cyber Security specialists only, but may synergize greatly if resources from other grouping are also included.
IT Provider	An IT provider provides services to clients and delivers a wide array of technology services such as security, disaster recovery services, management and support.

Terms	Definition
Logging solution	A logging solution provides organisations with data storage through centralised log aggregation. It improves security through a reduced attack surface, real time monitoring and improve detection and response times.
Multi factor authentication	Where a system requires a user to present a combination of two or more credentials to verify a user's login identity.
National Cyber Security Centre (NCSC)	Acts as a bridge between industry and government, providing a unified source of advice and guidance on cyber security.
NetSafe	NetSafe is New Zealand's independent, non-profit online safety organisation that provide online safety support, expertise and education to people in New Zealand.
Office of the Privacy Commissioner (OPC)	The Office of the Privacy Commissioner (OPC) is an Independent Crown Entity, financially supported by the state but operating free from government or ministerial control. OPC's responsibilities include issuing public statements on privacy issues, investigating privacy breaches, educating about privacy principles, assessing the impact of technology on privacy, reviewing legislation for privacy implications, receiving reports of significant privacy breaches, enforcing the Privacy Act, and reporting to the government on domestic and international privacy concerns.
Phishing	When cyber criminals try and trick you into giving them money, information, or access to your organisation's systems. For example, pretending that your bank account has been locked and you need to re-enter your credentials.
Privacy Act 2020	The Privacy Act 2020 governs how organisations and businesses can collect, store, use and share individual information.
Privacy Breach	A privacy breach incident occurs when personal information held by the organisation is accessed, disclosed, altered, lost, or destroyed without proper authorisation.
Protected Health Information	Health information that relates to the past, present or future health of an individual; the provision of healthcare to an individual or the payment for the provision of healthcare to an individual.
Ransomware	A type of malware that encrypts (locks up) your files so you can't access them. It can also completely stop your devices or system from working. Cyber criminals then ask you to pay money to get your files unlocked.
Root Cause	The process of finding the underlying source of a problem, so that a solution can be identified and implemented.
Threat Hunting	A proactive security search through networks, endpoints, and datasets to hunt malicious, suspicious, or risky activities that have evaded detection by existing tools.

Health New Zealand
Te Whatu Ora