Strengthen Your Digital Defence

A Guide to Cyber Security Incident Response for New Zealand Primary Health Sector

Stop! If you are currently experiencing a live cyber security incident, go to page 14 for immediate response steps.

Te Kāwanatanga o Aotearoa
New Zealand Government

Health New Zealand
Te Whatu Ora

Citation: Health New Zealand | Te Whatu Ora. 2025. *Strengthen your digital defence: A guide to cyber security incident response for New Zealand Primary Health Sector*. Wellington: Health New Zealand | Te Whatu Ora.

Published in May 2025 by Health New Zealand | Te Whatu Ora
PO Box 793, Wellington 6140, New Zealand

ISBN 978-1-991139-41-2 (online)

Health New Zealand
Te Whatu Ora

This document is available at **tewhatuora.govt.nz**

Contents

Acknowledgements

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 cyber security advice which holds real life experience and clinical priorities at its core.

Published November 2023 | Redesigned May 2025

1 Introduction

Cyber security incidents are becoming increasingly frequent in the healthcare sector. These incidents often disrupt critical service delivery and lead to the **loss of health information**, which healthcare providers have a **regulatory and moral obligation to protect**.

It is not a case of 'if' but 'when' your organisation will experience a cyber security incident.

This booklet provides **guidance for primary health sector organisations** on how to prepare and respond to the worst-case incidents.

This booklet is part of an information toolkit developed by Health New Zealand and it is not intended to be an exhaustive source of advice. Visit the '**Cyber Hub**' for further supporting resources.

Some factors that make the risk of cyber security incidents worse for small health organisations include:

The average cost of a data breach in healthcare has increased by 42% since 2020.[1]

Research shows that small businesses are 3x more likely to be targeted by cyber criminals than large businesses.[2]

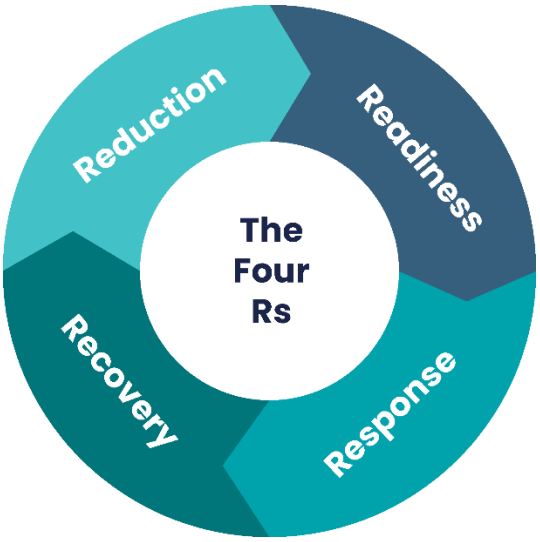
Protected Health Information (PHI) sells for 50x more than other personally identifiable information (PII) on the dark web.[3]

If you'd like to learn more, our sources are referenced at page 22 along with links to further reading and resources.

2 Cyber Security and The Four Rs

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. They are **unauthorised events that compromise computer systems, data, or networks and potentially causes harm.**

Follow the "Four Rs": **Reduction, Readiness, Response and Recovery** as guidance to break down the steps you need to follow to **prepare for and respond to a cyber security incident**.



Reduction

Prepare your organisation before a cyber attack occurs by **reducing cyber security risks** to reduce the impact and the likelihood of a incident.

"Research shows that organisations with **good cyber hygiene are 7 times less likely** to have a publicly reported breach event relative to those with 'poor' cyber hygiene."[4]

Readiness

Be ready to respond to an incident by **educating** your workforce, and creating an **Incident Response Plan**.

"In 2023, **74% of breaches** in the healthcare sector involved the **human elemen**t."[5]

Response

A quick and **decisive response** helps to effectively **contain and remediate** the threat. This is critical to prevent further damage in the long and short term.

"Research shows with a tested cyber security plan you could **significantly reduce** the cost of a cyber security breach."[6]

Recovery

Recover your systems, devices and data effectively once the cause has been remediated. **Learn** from the experience and what you would do differently.

"In 2022, the average hospital took 287 days to fully recover from a ransomware incident."[7]

2.1 Reduction

Take the time to understand your organisation's digital environment so that you can prioritise securing **critical assets** (i.e. your IT systems, devices and data) and **reduce the risk** of a significant disruption and loss of patient data.

You can reduce the risk of a cyber security incident by following this three step plan:

Step One: Identify your most critical assets. Outline the following

Which tools are essential for daily work?

- Include physical devices (laptops/servers) and software (patient management systems).
- Which systems hold confidential PHI, PII or critical service data?
- What digital connections do you have with third parties?

Include:

- Wider healthcare services you receive or supply data to.
- Any IT service providers who have access to your systems or provide services.

Step Two: Prioritise those assets based on service criticality and risk:

- How long could our organisation function without the asset?
- Does the asset hold critical data or PHI?
- Is the asset connected to other critical systems, devices or data?
- What would the impact be on service delivery?

Step Three: Manage the risk to your most critical assets:

- Discuss cyber security risk during organisation management meetings.
- Create and test Business Continuity Plans (BCP) and Disaster Recovery (DR) plans.
- Review what foundational cyber security controls (example list overleaf) are in place.
- Talk to your IT staff or vendor(s) to agree on their responsibilities for DR and cyber security controls.

Business Continuity Plan (BCP)

BCPs are documented procedures that organisations follow to respond, recover, resume, and restore to a pre-defined level of operation following disruption.

Disaster Recovery (DR) Plan

A DR 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.

Protect your business from a cyber attack by improving your cyber security hygiene. Follow the checklists below to understand what you can do within your organisation, and what you should work with your IT provider to complete.

IT Provider Response Checklist:

Work with your IT provider to understand how they will:

A. Prevent data loss by:

- Backing up critical systems regularly
- Keeping backups offline or in the cloud
- Testing backups

B. Eliminate known vulnerabilities:

- Regularly install system and hardware updates for applications, web browsers, and operating systems

C. Detect a cyber security incident through the use of the following tools:

- Endpoint Detection and Response (EDR)
- Logging solution
- Antivirus software
- Firewall and web application firewall

D. Respond to an incident:

- Do they provide cyber incident response support as a part of your service agreement, including coverage of cyber incident triage, investigation and root cause analysis?

- How will they notify you when a security incident is detected? This should be written into the contract you have with your IT provider
- Do they utilise threat hunting tools and techniques for cyber incident response?
- Will they provide comprehensive incident reports including analysis findings and recommendations?

Organisation Response Checklist:

Complete this as a minimum for basic internal cyber hygiene.

A. Provide cyber education and awareness to employees so they are able to:

- Recognise a phishing scam
- Report suspicious activity to the right channels
- Promote a culture of cyber awareness internally

B. Control and monitor access to devices, systems and files:

- Only give authorised employees access to systems and data they need to carry out their jobs
- Enable Multi Factor Authentication (MFA) on critical systems (e.g. those that hold critical services data or PHI)
- Encourage the use of long, strong passwords, and ensure they are changed regularly

C. Risk assess any IT providers that have access to your data, provide critical services or are connected to your IT environment by:

- Knowing who your providers are and what services they support
- Identifying those that are most critical or have access to PHI
- Setting minimum security standards that must be met
- Seeking legal advice about compliance requirements may be beneficial

An ‘IT provider’ could be in-house or a third party that provides IT support or manages your IT hardware or systems.

2.2 Readiness

An Incident Response Plan is a written document that will help your organisation before, during and after a confirmed or suspected cyber security incident. **Prepare and practice** your response plan before an incident occurs.

You should include the following in your Incident Response Plan:

A. <u>Roles and Responsibilities:</u>

Identify who can help out in an incident and what their **roles and responsibilities** will be. Sometimes people may have to wear more than one 'hat' to get the job done.

Important roles you should include are:

- An **Incident Lead** from the organisation who understands the business and is accountable for decision-making
- A **Technical Liaison** who manages communication between your organisation and the technical IT response
- A **Communications Lead** who writes and shares communication messages to stakeholders and impacted individuals
- A **Legal Advisor** who can provide legal and insurance advice

B. <u>Incident Severity Level</u>

Define **incident severity levels** so that response efforts are proportionate to risk and impact to your organisation.

C. <u>Escalation Pathways</u>

Define when and to whom an **incident needs to be escalated to make sure those that can help you are able to do so**.

Escalation criteria could include notification to business management, board members, regulatory bodies and government agencies. These include (but are not limited to):

The **Office of the Privacy Commissioner** – this is a requirement if you believe you have had a data breach that could cause serious harm

- **CERT NZ** who may be able to provide technical support
- Your **insurance provider** should be engaged early (where applicable)
- **NZ Police** as a crime may have been committed
- Your **IT provider(s)**

D. <u>Stakeholder Communications</u>

Document a **clear communications plan to notify all relevant stakeholders**. Patients, staff and third parties are key stakeholders who will require communication throughout the incident response and recovery.

Think about some different scenarios that could occur and what your key messages might be? For example:

- A ransomware attack means you cannot access any patient management systems. How will you notify patients to changes in appointments?
- PHI has been stolen. How will you identify and notify affected patients, as well as the Office of the Privacy Commissioner?

Top Communication Tips:

1. Seek legal advice if able to do so
2. Prepare draft statements in advance
3. Identify the communication method(s) you will use during incidents
4. Keep messaging factual and balanced
5. Communicate regularly and at agreed times, even if there is nothing new to share
6. Plan and provide advice to those affected
7. Avoid promising resolution before the incident is understood
8. Remember that internal communications could be leaked to the public
9. Consider the risk to your organisation's reputation when making statements

Keep a copy of your incident response plan 'offline', for example stored on a secure USB drive

E. Essential response activity:

You can't plan for everything you'll need to do during a cyber security incident. But as a minimum, there are some standard activities that you should include in every response:

- **Set your guiding objective** – this aligns your team with a common goal.
- **Hold regular response meetings** – helping to coordinate activity and manage risk in a structured way.
- **Maintain detailed documentation** – comprehensive records like meeting minutes and decision/action registers are important evidence around what occurred, and may be required for audits or insurance checks.
- **Put welfare on the agenda** – don't forget to check in with your staff on how they are feeling and support they may need.

F. Practice:

Once you have an Incident Response Plan in place, schedule regular walkthroughs of your plan to practice with key staff members and IT providers. This offers an opportunity to train, develop muscle memory and improve the process.

Unexpected lessons from a recent cyber incident…

*The most important thing for us was our **insurance claim**, we're still doing the paperwork but it saved our organisation from going under…*

*Our incident is wrapped up, but we still get messages from **people who are worried** that a hack in their personal life might be related to what happened…*

2.3 Response

Use this process flow for a step by step guide to respond to a cyber security incident.

This response process can be used as a pull out for ease of reference in an active incident

Incident detected

Step Number	Business Response Steps	Technical Response Steps
1	Notify your IT provider and validate whether this is a cyber incident	
2	Activate your Incident Response Plan	
3	Assess the impact on the business to determine the severity of the incident. • Has data been stolen or breached? • Are critical systems or devices unavailable?	Keep communication open between the business and IT response to understand impact, where additional help may be needed and who else may need to be communicated with as the response develops

Is this a critical incident?

- No – Manage internally with IT provider
- Yes – Continue to step 4

4	Decide who you need to support the response. • Decide who can support your response. This could include your cyber insurance provider, legal advisor and CERT	Investigate the extent of the incident • Find out why and how the incident happened • Preserve evidence and keep any valuable information
5	Initiate your Business Continuity Plan (BCP)	Stop the spread/mitigate the impact • Mitigating actions could include:

	• A prolonged incident could stretch your manual processes • Consider what additional resource and support your staff may need	• Shutting down systems and changing passwords • Disconnecting from compromised networks • Make decisions with awareness of the impact this will have on service availability for you and external stakeholders • Communicate to those impacted
6	Assess whether you need to notify any external stakeholders or regulatory bodies. Deliver communication messages as appropriate • Keep messaging factual and balanced • Avoid promising resolution before the incident is understood • Remember that internal communications could be leaked to the public	Remediate the source of the incident • Fix vulnerabilities by patching any weaknesses or security threats • Remove any harmful elements such as malicious files or malware • Increase monitoring to make sure you are not reinfected

Has the threat been remediated?

- No – Repeat from step 4 (re-investigate)
- Yes – Continue to step 7

7	Debrief and identify lessons learnt • Create an action plan to improve readiness and response • Involve everyone who assisted with the response when identifying lessons learnt	Recover systems, devices and data • Initiate applicable disaster recovery plan(s) • Restore systems in a prioritised, risk based way

Incident Closed

- If you have cyber incident insurance and legal counsel engage your provider(s) early.
- You should notify the Office of the Privacy Commissioner (OPC) within 72 hours if you believe you have had a data breach that could cause serious harm.
- Notify CERT NZ for support in responding to the incident.

2.4 Recovery

Completing the recovery process in full is essential to return to normal operations and **limit damage to your business**. Remember, some recovery steps will take longer than others. Recovery activities need to be completed by both your IT provider (s) and your health organisation.

IT Provider Response Checklist:

A. Confirm the root cause of the incident:

- What is the root cause of the incident?
- Has the threat been eliminated?
- If the root cause has been confirmed, secure backups from before the incident can help with service restoration

B. Make sure you thoroughly patch systems:

- Apply necessary updates to fix vulnerabilities before reconnecting systems and devices

C. Prioritise restoration of critical information:

- Prioritise the restoration of critical patient data
- Prioritise the restoration of vital systems

D. Continue security measures:

- Continuously watch for suspicious activity or signs of recurring incidents
- Enhance security controls for backup infrastructure to prevent unauthorised access

Organisation Response Checklist:

A. Hold a 'Lessons Learned' discussion with all those involved as soon as possible to review what happened.

B. Make an improvement plan.

- Write down the actions that were identified during the debrief
- Create a plan to address those actions
- Assign responsible individuals to each action so they can work on improving them

C. Build back trust.

- Consider how you will continue to support those impacted (for example, your patients, the community and your staff)

D. Regularly update and test backups.

- Keep your backups and recovery processes reliable by regularly updating and validating the effectiveness of the restoration and recovery procedures

Recovery takes time – an incident will impact your business functions, reputation, finances and the community.

Make a recovery plan that considers all of these elements.

3 Appendices

3.1 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 Office of the Privacy Commissioner** within 72 hours. The Office of the Privacy Commissioner 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 here.
- 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 provides information and advice to the New Zealand health sector about cyber security, including tools and templates. Te Whatu Ora 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 cyber security incident response and resilience:

- 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 – **top tips for cyber security** – a useful infographic on basic, personal cyber security hygiene.
- 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.

3.2 References

1. ***IBM Cost of a Data Breach Report 2023***, Written by Ponemon Institute and IBM Security, July 2023, Cost of a data breach 2023 | IBM.

2. ***Forbes: Small Businesses are More Frequent Targets of Cyberattacks than Larger Companies: New Report***. Written by Edward Segal, March 2022, Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report (forbes.com).

3. ***Healthcare IoT Security Operations Maturity, A Rationalised Approach to a New Normal***. Written by Crowdstrike and Medigate, ReportCSMedigateHealthcareIoTSecurityOpsMaturity.pdf (crowdstrike.com).

4. ***Harvard Business Review: The Devastating Business Impacts of a Cyber Breach***. Written by Huang, Wang, Wei and Madnick, May 2023. The Devastating Business Impacts of a Cyber Breach (hbr.org).

5. ***2023 Data Breach Investigations Report: Healthcare Snapshot***. Written by Verizon 2023, Small Businesses Data Breach Investigations Report

6. ***IBM Report: Half of Breached Organisations unwilling to Increase Security Spend Despite Soaring Costs***, Written by IBM Security, July 2023, IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs.

7. ***IBM Cost of a Data Breach Report 2023***, Written by Ponemon Institute and IBM Security, July 2023, Cost of a data breach 2023 | IBM.

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.
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.

Terms	Definition
Incident Response	The effort to quickly identify an attack, reduce its effects, contain damage and remediate the cause to reduce risk of future incidents.
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.
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.
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.
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.

Notes

Te Kāwanatanga o Aotearoa
New Zealand Government

Health New Zealand
Te Whatu Ora