Medical Protection

WellSouth 11 February 2026

Hot topics: Learnings from MMH 12 Month scripts

Dr Sam King GP and Medicolegal Consultant MPS

Learnings from MMH Cyber-attack

Manage My Health cyber-attack

- Hack occured 30 December 2025
- 31 Dec MMH confirmed breach
- Delays in finding out which patients affected, communication with practices
- Despite practices ending contract, MMH still held data and for some patients, were still uploading data

Who is the agency?

(a) Privacy and data protection regulation in New Zealand works on the concept of a responsible agency. Where you are the relevant agency for personal or health information you are responsible for that information. It is your job to ensure it is appropriately secured, that it is only used in line with the Privacy Act of Health Information Privacy Code, and that notifiable data breaches are investigated a notified appropriately.

(b) Where personal information is stored or processed on your behalf you remain the agency – so while data may be held on someone else's systems you remain responsible for it.

Who is the agency?

c) When engaging with third parties who host or process patient data on your behalf the first question should be – who is the agency? Is the practice still the agency? Or has the third-party vendor taken over that role? What does the contract say? Where does responsibility lie?

What does the third party provider do with the information you provide?

a) Are there limitations on what they can do with the information? Are these specified in the contract? Can they use if for their own purposes as well as storing or processing it on your behalf?

b) Does the contract set out how the third party provider will assist you in responding to access requests by patients, deleting information when patients move on, or uplifting your data and moving to a new provider if you choose to terminate the contract?

c) Are retention periods implemented? Is data deleted after a certain period of time?

What security measures are in place?

a) If you are the agency you are required to ensure that appropriate security measures are in place. This remains the case even when information is held by a third party provider on your behalf.

b) Does the contract require that appropriate security measures are in place? What are they? Are they updated?

c) How can the provider prove to you that they have appropriate security in place? Do they have any third party verification? Is there any third party quality control or checks in place? Is security overseen or tested by external experts? How regularly does this occur?

What security measures are in place?

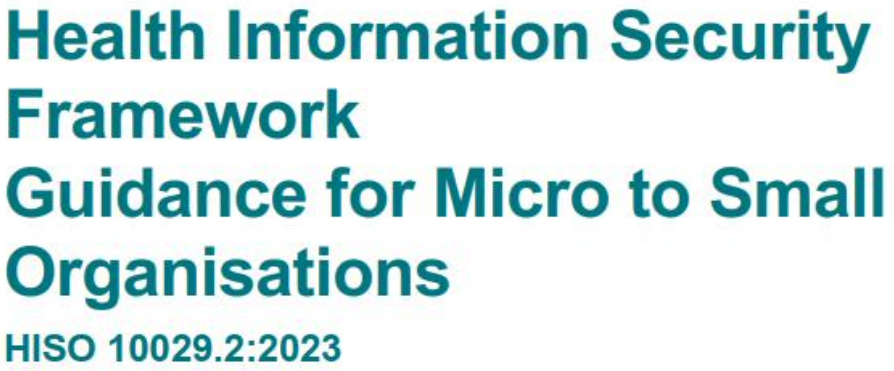
a) Have they considered the Health Information Security Framework (HISO 10029:2022) and the controls referred to within?

https://www.tewhatuora.govt.nz/health-services-and-programmes/digital-health/data-and-digital-standards/health-information-standards-organisation-hiso#security-standards

https://www.tewhatuora.govt.nz/health-services-and-programmes/cyber-hub/cyber-security-resources-for-primary-healthcare-providers

hiso Health Information Standards Organisation PAEREWA PARONGO HAUORA

Te Whatu Ora Health New Zealand



Consent

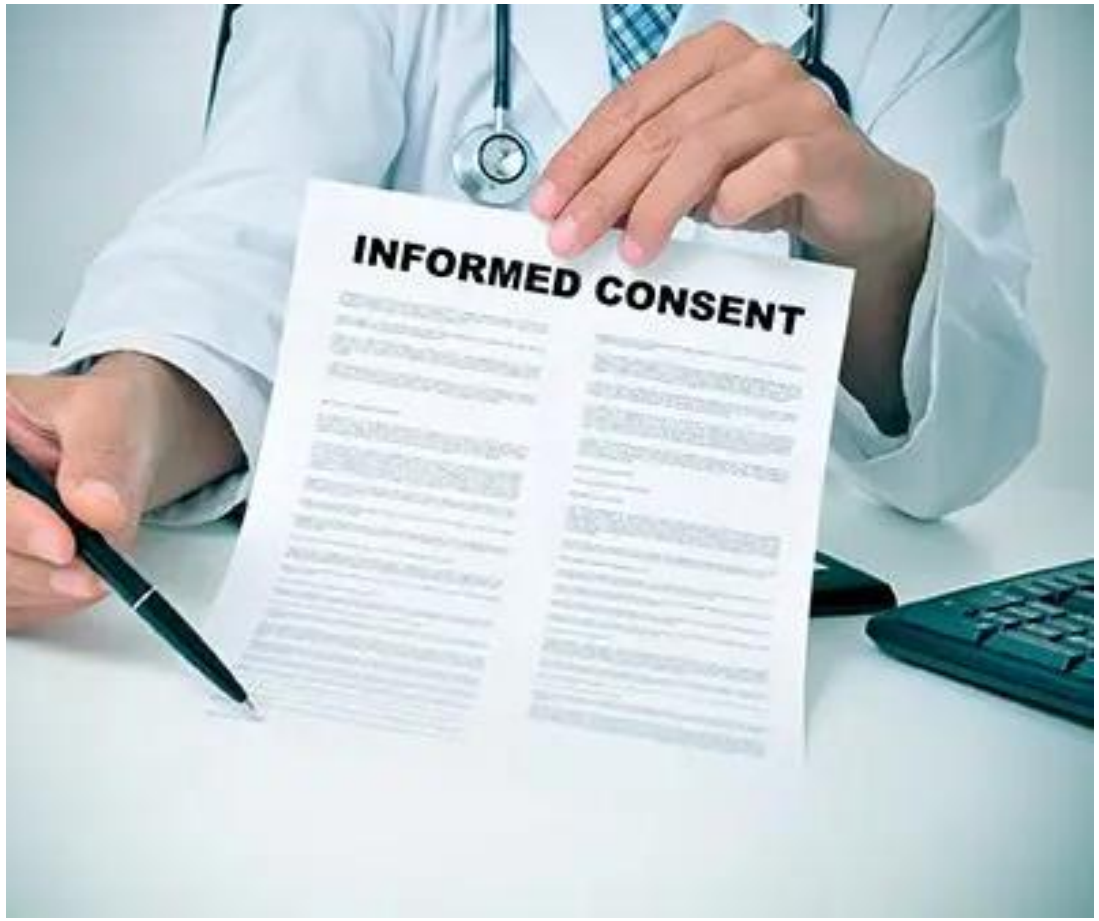
a) What information has been provided to patients? Patients have a right to know who the third party are, where they are, if the information is held offshore. Who has access, is it used for any other purpose?

b) Consider presenting this in diferrent ways: verbal, written, video.

c) Do need the information in different languages?

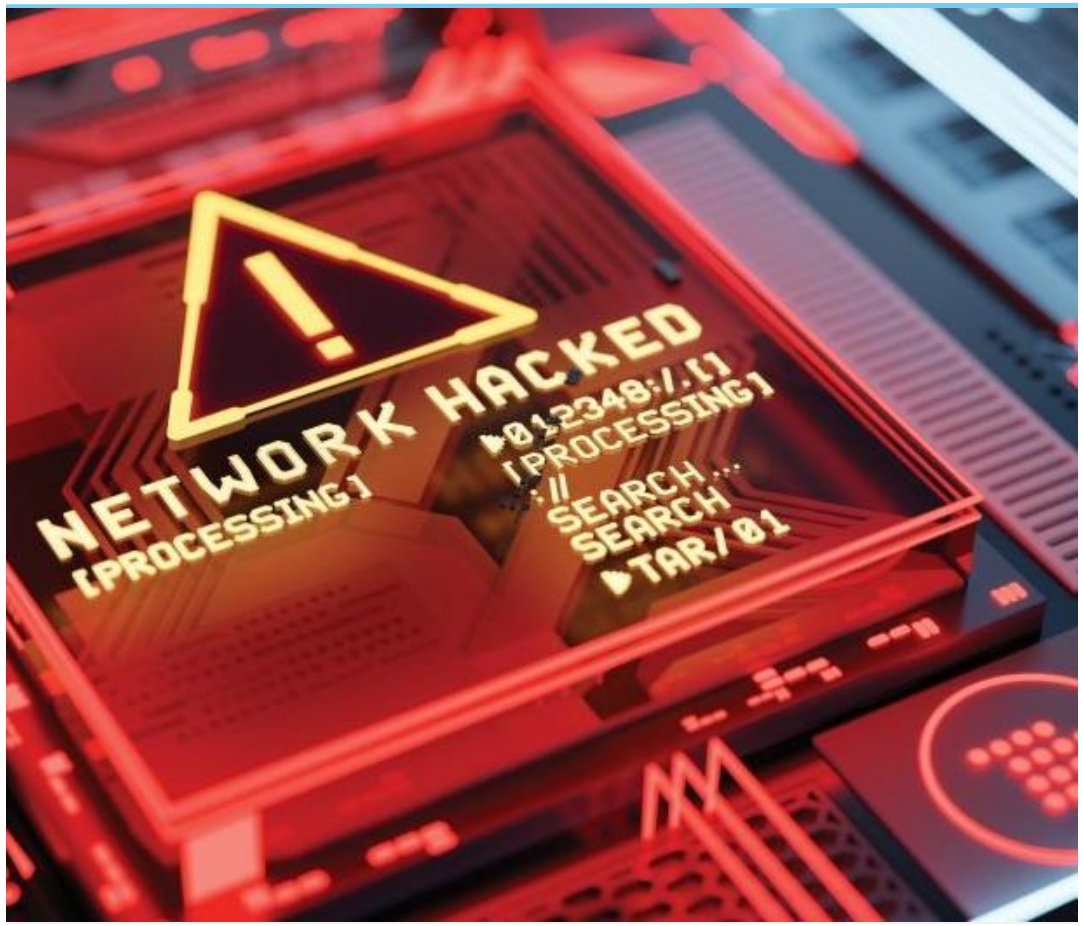
d) How can you check understanding?

e) Keep a record of consent.



Following any breach

a) Contain the breach
b) What happened
c) What specific information has been released
d) How it happened
e) What should have happened
f) What you are going to do to minimise risk of recurrence
g) Which patients need open disclosure
h) When to disclose
i) Where can patients find out more information
j) Do you need to notify the Privacy Commissioner‘s Office? NotifyUs tool



What happens when there is a breach?

a) The Privacy Act 2020 requires that **agencies notify individuals** where there has been a notifiable privacy breach. There is **no requirement, however, that those hosting or processing personal information on behalf of agencies** notifying the agency if they have an incident. This can create a difficult situation where personal information you are responsible for has been impacted in a data breach, but the entity actually holding it has **no obligations to tell you or do anything about it**. In those circumstances you are reliant on the **terms of your agreement** with the third party provider.

What happens when there is a breach?

b) What notification obligations are contained in the contract? Is the third party provider required to notify you if there is a security incident? Is there a timing requirement that will give you sufficient time to inform the likes of the Office of the Privacy Commissioner? Is the provider required to investigate the incident and provide necessary support to the practice in responding to the incident? Who bears the cost of doing so?

c) Liability – does the contract specify who is liable if there is a notifiable privacy breach and costs are incurred/individuals seek compensation? Is there a limitation of liability clause that would prevent the practice recovering against the third party provider?

Third party cyber incident

a) How is the third party responding? Have they confirmed the breach has been contained? Has this been verified by a third party specialist, or is the provider effectively marking their own homework? Is it safe to keep engaging with them/provide more information, or should access be cut off?

b) What steps are being taken to verify what personal or health information may be impacted? This can take some time and typically should involve an external digital forensics expert. Many software platform providers consider themselves knowledgeable enough to conduct such analysis, but this is a specialist area that requires a specialist digital forensics provider.

c) How regularly is the provider going to update you, and what information are they going to provide? Are they providing enough information to pass on to your community about what has happened? Are you better off waiting and communicating to your community once you know more?

Third party cyber incident

d) Who is required to make notifications to the Office of the Privacy Commissioner and individuals as a matter of law? Or put differently, who is the relevant agency? Has the notification threshold (likely to cause “serious harm”) been met? We note that notification obligations are an area where advice from a privacy lawyer can be helpful.

e) Legalities to one side, who is practically best placed for make any necessary notifications? For example – if a platform provider suffers an incident impacting many practices, is it best that the platform provider notifies the OPC on behalf of all the impacted practices?

f) Who is going to support notifications? If impacted individuals have questions should those go to the practice, the third party provider, or another specialist provider like IDCare?

Anxious patients

Some patients who have sensitive information (perception is in the eye of the beholder) will contact the practice very anxious.

- Open disclosure or not?
- MMH breach is very public, consider their risk of self-harm
- Support people

Communicating with your patients

What needs to be communicated and to who? Do you contact all patients or only respond to the ones who contact the practice?

Does the practice make the disclosure or do you allow the third party to do so, as in the MMH case?

Check your own security in order to reassure your patients.

Final lessons

a) When the contract ends what happens to the information?
b) Check that information is not accessible for uploading
c) Check your own security

12 month prescriptions

Te Kaunihera Rata o Aotearoa | Medical Council of New Zealand

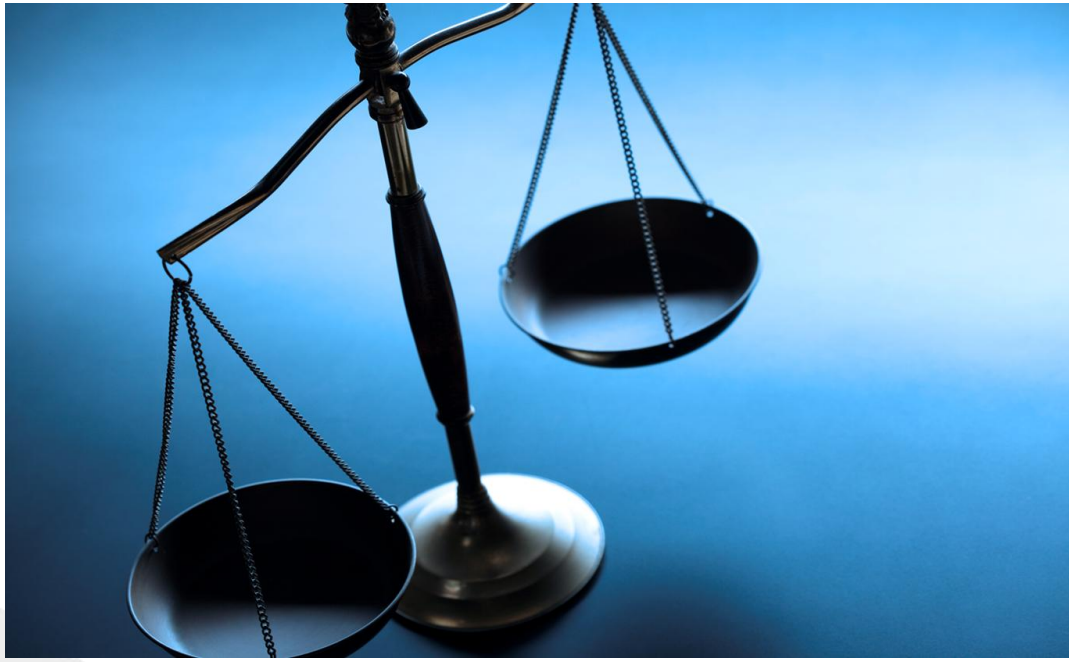
February 2024

www.mcnz.org.nz

Good prescribing practice

- "… You should only prescribe medicines or treatment when you have **adequately assessed the patient's condition**, and/or have **adequate knowledge** of the patient's condition and are therefore satisfied that the medicines or treatment are in the **patient's best interests**.
- **Never prescribe indiscriminately, excessively or recklessly**…
- **Periodically review** the effect (benefits and harms) of the treatment and any **new information about the patient's condition and health if the treatment is being prescribed for an extended period of time…**"

How does the clinician decide?



Individual clinical decision dependent on:

- Patient age and cognitive function
- What medical conditions and how many
- What and how many medications
- Health literacy
- Compliance with the medication, blood tests etc

Practice policy

- Policies protect the practice more than clinicians
- If you dont have one write one
- Are there medications that are never longer than 3 months?
- Are there medications that are always 12 months? (unlikely)
- Principles to guide prescribers rather than rules
- Does the patient have to return for an appointment at the end of the 6/9/12 months?
- Ensure good documentation by the staff
- What if patient doesn‘t come for follow up as advised?

Avoiding complaints

- Emphasise patient safety as the prime focus
- Educate the patients
- Patient pamphlets, emails, website update
- What increased responsibility must the patient be aware of?

Patient pressure: You will not be vulnerable to complaint if you do the right thing and the patient complains. If there is an adverse outcome you will be in trouble if you‘ve done the wrong thing.

Medical Protection

Questions??

Medical Protection

Listen and subscribe to our podcasts

The Medical Protection podcasts discuss key and current medicolegal risks and issues affecting clinicians across Aotearoa New Zealand.

Medical Protection