## AFFECTED PATIENTS FAQ

Version dated 5pm 7 Jan 2025

1. I would like you to remove any health documents you have stored in the cloud, but I still want to keep my MMH account.

Manage My Health currently stores information as part of a single patient account. We are not able to selectively remove cloud storage while keeping all account functions active. If you wish to remove stored documents, you can choose to delete documents you uploaded or close your account entirely. If you close your account, your data will be deleted in line with our processes.

2. I am requesting all my personal data under the Privacy Act 2020 and want it provided in an encrypted file. I also want an update on the breach and want my account closed and data deleted.

You have the right to request access to your personal information under the Privacy Act 2020. Requests for personal data, breach updates, and account closure should be submitted through Manage My Health support. These requests are handled in line with legal timeframes. Once an account is closed, data is deleted through platform processes.

3. What type of information was involved?

The incident relates to documents stored in the My Health Documents section. These are documents that users uploaded themselves, such as correspondence, reports, or results they chose to keep for their own records.  It also includes Hospital Discharge summary documents for Northland hospital (including clinical letters and other documents that patients receive from hospital clinicians).  The final set of documents are specialist referral letters from GPs to Specialists for the years 2017-2019. This did not include GP clinical systems, prescriptions, secure messaging, or appointment systems.

4. Can I access my medical records safely?

Yes. The current system environment has been confirmed as secure and operating as intended. Access to your account is safe.

5. Does this breach affect my GP, clinic, or hospital records?

No. GP clinical systems, hospital systems, prescriptions, secure messaging, and appointment systems were not affected.

6. Can MMH guarantee my data will not be misused?

Manage My Health has taken steps to secure the system and prevent further unauthorised access. Like all digital platforms, no system can provide an absolute guarantee, but safeguards and monitoring are in place.

7. What if I no longer want to use MMH?

You can choose to close your account at any time. When an account is closed, data is deleted through platform processes.

8. Can I reopen my account later if I close it now?

If you close your account, it is deleted. You would need to create a new account if you choose to use Manage My Health again in the future.

9. Will MMH compensate affected patients?

At this stage, Manage My Health is focused on notifying affected individuals, providing support, and meeting its legal obligations. Compensation matters are assessed on a case-by-case basis in line with applicable law.

10. Has anyone been held accountable for this incident?

The matter is under investigation. It would not be appropriate to comment further while investigations and legal processes are ongoing.

11. Can I request MMH to delete specific information only?

"Yes, you can delete the documents held in the 'My Health Documents' folder. Go to the folder and follow the prompts to delete the files. To delete all your information in MMH close your account by going to My Account -> Close Account"

12. What has MMH done to secure the system?

The affected feature has been secured, independent cyber security specialists engaged, regulators notified, and additional safeguards implemented.

13. What changes has MMH made to prevent this happening again?

MMH has reviewed controls around document access, strengthened monitoring, and implemented additional security measures to reduce the risk of similar incidents.

14. Do I need to contact my GP or practice?

No. You do not need to contact your GP or practice regarding this incident unless they advise you to do so.

15. Where can I get independent advice?

You may seek independent advice from the Office of the Privacy Commissioner, Netsafe, or a legal adviser.

16. What if my practice no longer uses MMH?

You may still have an MMH account even if your practice no longer uses the platform. Accounts belong to patients and remain active unless you close them.

17. What should I do if I believe my information has been misused?

Do not engage with anyone making threats or demands. Contact New Zealand Police immediately and report the issue to Manage My Health using the support details provided.

18. How do I know if an email or message is really from MMH?

Official messages from Manage My Health will not ask for your password or payment details. If you are unsure, contact MMH support directly using official contact details.

19. Do I need to change my MMH password?

As a precaution, you may choose to change your password, especially if you reuse passwords across other services.

20. If I close my MMH account, will my data be removed from hackers' access?

Once an account is closed, data is deleted through platform processes. The system environment has been secured to prevent further unauthorised access.

21. Has the Privacy Commissioner been notified?

Yes. The Office of the Privacy Commissioner has been notified, and Manage My Health is working with Health New Zealand and other relevant agencies.

22. Should I close my account?

This is a personal decision. Manage My Health continues to operate securely, and many patients choose to keep their account for access to services.

23. Why did it take time to notify patients?

Notifications began once forensic confirmation was available and support mechanisms, such as the 0800 number, were in place to assist patients properly.

24. Was any of my financial or banking information involved?

No. Financial or banking information was not involved.

25. Was my password accessed?

There is no evidence that passwords were accessed as part of this incident.

26. Should I be concerned about identity theft?

Manage My Health has partnered with IDCARE, Australia and New Zealand's identity and cyber support community service.
If you are concerned about any potential or actual identity theft as a result of the incident, Manage My Health suggests that you get in contact with IDCARE as they can provide further recommendations which are tailored to you.

Please be aware that IDCARE are unable to assist with any health information concerns you might have. IDCARE can only assist with identity compromise and misuse.

IDCARE's services are at no cost to you.

If you have any identity documents or credentials that have been compromised or you are experiencing misuse of your identity, please complete an online Get Help form at www.idcare.org and IDCARE's expert Case Managers will get in contact within operating hours (Monday to Friday 10am-10pm NZDT excluding public holidays).

When engaging IDCARE, please use the referral code **MMH26.** This code is unique to you and should not be shared with anyone other than Manage My Health and IDCARE.