FAQs for Patients | ManageMyHealth Incident

9 January 2026

You may have seen news about a cyber security incident involving the **Manage My Health** patient portal.

That incident is not connected to our practice's myindici patient portal service.

1. **Is our practice affected by the Manage My Health incident?**

   No. The Manage My Health incident relates to a different provider and platform. The myindici patient portal is separate and was not involved.

2. **Who owns and manages my health information?**

   Your health information belongs to you. Our practice is responsible for holding and managing your health record as part of your care, including responding to requests to access or correct information, in line with our legal obligations and policies.

3. **Can I ask the software provider to change or delete my information?**

   No. Our myindici patient portal is made available to you through our practice. Requests to access, correct, or delete information must be managed by our practice. The software provider cannot accept or action patient requests directly.

4. **What should I do if I want to correct something in my record?**

   Please contact our practice. We will guide you through the appropriate process to request a correction.

5. **Can you tell me exactly what security measures are in place?**

   We use a healthcare software provider to deliver our myindici patient portal for use by our patients. The detailed security and privacy arrangements (including technical controls and contractual commitments) sit within a confidential agreement between our practice and the provider.

   For security reasons, we do not publish detailed security controls publicly, because that can undermine security by providing useful information to bad actors. What we can reassure you is that protecting patient information is treated as a critical responsibility. Our software provider maintains an active security and privacy programme that is regularly reviewed and improved over time, and our practice also maintains appropriate governance and processes around how patient information is managed.

   While no technology can be guaranteed to be risk-free in all circumstances, we and our software provider take all reasonable precautions and work continuously to reduce risk as threats evolve.

6. Should I contact the software provider if I have security questions?

No. Please contact our practice instead.

We (the practice) have the direct relationship with you as our patient. Our software provider does not have a direct relationship with patients and does not handle patient security enquiries. For security reasons, detailed security information is not discussed publicly.

7. Is the portal "100% secure"?

No technology (not just clinical systems) can be guaranteed to be impenetrable at all times. Any "cast iron guarantee" would be misleading and irresponsible. What matters is that strong safeguards are in place, that security is treated as an ongoing process, and that issues are responded to quickly and appropriately.

8. What is the status of my information before I moved to myindici?

It depends on which "before" situation applies:

(a) **Before you joined our practice** - any health information created while you were enrolled with a different practice is held by that previous practice (or provider). It is not automatically transferred to us or into myindici just because you later joined our practice.

(b) **Our practice previously used Manage My Health** - moving from Manage My Health to myindici does not automatically move, delete, or change information held in Manage My Health (or any other previous system). Some historical portal-related information may remain with Manage My Health and/or the previous system, depending on what was stored there and the arrangements in place at the time.

If you want to know what information is still held in Manage My Health, you should check with Manage My Health directly.

9. What can I do to protect myself online?

- Use a strong, unique password (do not reuse passwords across sites).
- Be cautious of unexpected emails/texts/calls asking for personal information or logins.
- Never share your password with anyone (including anyone claiming to be from a health service).
- If you are unsure about a message that appears health-related, contact our practice using our official contact details.

10. I received a suspicious message - what should I do?

Do not click links or provide information. Contact our practice and we will help you confirm whether it is legitimate.

11. Who can I contact if I am concerned?

We understand that reports of cyber incidents can be worrying. For most patients, no action is required.

If you believe there is an urgent issue - for example, you notice suspicious activity on your account, receive a message asking for passwords/one-time codes, or think your information may have been misused - please contact our practice using our usual contact details.

Please do not contact our technology provider directly; the practice manages all patient enquiries and requests about health information.