Fact sheet

Passphrases and multi-factor authentication

Healthcare services manage sensitive health and personal information and rely on secure access to clinical, administrative and communication systems.

Strong passphrases and multi-factor authentication (MFA) help protect patient information, business systems and staff accounts from unauthorised access and cyber threats. For practices, clinics and other healthcare providers, these measures lower the risk of privacy breaches, service disruption and fraud; while helping staff access the systems they need safely each day.

If an attacker gains access to an account, the result can include data breaches, operational delays, financial loss and reduced trust. The Australian Cyber Security Centre[1] describes MFA as one of the most effective controls to prevent unauthorised access, and Office of the Australian Information Commissioner[2] highlights strong credential practices as an important way to reduce data breach risk.

What is a passphrase?

A passphrase is a long password made from 4 or more random words. It is easier to remember than a complex short password and is generally harder for attackers to guess or crack using automated tools.

How to create a strong passphrase

- Use at least 4 random words and aim for 15 characters or more.
- Avoid names, birth dates, clinic names, common phrases or predictable patterns.
- Use a different passphrase for each important account, especially email, remote access and business-critical systems.
- Store passphrases securely using approved tools or processes and never share them.

Passphrase example: riverteacupplanetlantern.

Passphrase example with extra complexity: River7-Teacup!Planet-Lantern42.
(Apply if a system requires extra complexity such as capital letters, numbers or special characters without losing the randomness of the words)

What is MFA?

Strong passphrases and MFA work best when used together. A strong passphrase helps protect an account, while MFA provides an additional layer of protection if a passphrase is stolen or guessed. Instead of relying only on a username and passphrase, staff must also provide another form of verification such as an authenticator app code, security token or biometric check. The Australian Cyber Security Centre[3] recommends phishing-resistant MFA where possible because it offers stronger protection than relying on passwords alone or weaker methods such as SMS.

[1] Implementing multi-factor authentication | Cyber.gov.au
[2] Guide to securing personal information | OAIC
[3] Implementing multi-factor authentication | Cyber.gov.au

Practical actions

- Use strong, unique passphrases for business systems and administrator accounts.
- Turn on MFA for email, remote access, cloud services, finance and any other system that holds sensitive information.
- Prioritise stronger MFA methods such as authenticator apps, security keys or biometrics where supported.
- Train staff to recognise phishing and never approve unexpected login prompts.
- Review access regularly and remove unused accounts promptly.

Common mistakes to avoid

- Reusing the same passphrase across multiple accounts or systems.
- Using predictable words, dates or names linked to your business or staff.
- Relying on passphrases alone for critical or remote access.
- Approving MFA prompts without checking whether the login attempt is expected.

If a passphrase has been compromised

If you suspect a passphrase has been exposed, compromised, reused on a breached service or shared with the wrong person, change it immediately. Update any reused passphrases on other accounts, review recent account activity, and report the incident through your cyber security team or IT support process. If MFA is not already enabled on the affected account, turn it on as soon as possible.

Strong passphrases and multi-factor authentication are simple but powerful steps healthcare services can take to reduce cyber risk and better protect patient information, staff accounts and essential systems. By using unique passphrases, enabling MFA and responding quickly if credentials are compromised, services can strengthen everyday security and help prevent avoidable incidents.