ERMS Login Upgrade – Important Information | Quick Help Guide

Overview

ERMS is upgrading its login system to **Microsoft Entra**.

This change improves security, simplifies access, and aligns ERMS with modern healthcare authentication standards.

This document explains **what is changing, why the change is happening**, answers **common questions** and assists with **installing authenticator apps**.

Who This Applies To

This change applies to ERMS users who **do not** use a Pegasus Health or CDHB/WCDHB Microsoft account.

If you use a Pegasus Health or CDHB/WCDHB Microsoft account, specific instructions apply.

What's Changing?

As part of the upgrade:

- You will receive a new ERMS Login ID (sent via email)
- You must reset your password before first use
- Multi-Factor Authentication (MFA) will be required
- You will be asked to accept a new ERMS Access Agreement after your first successful login

Why Are We Making This Change?

This upgrade allows ERMS to:

- Strengthen account and patient data security
- Reduce the risk of compromised passwords
- Provide a consistent login experience across:
  - Web browser access
  - Practice Management Systems (PMS)
- Meet current healthcare security standards

About Multi-Factor Authentication (MFA)

What is MFA?

MFA adds an extra layer of security by asking you to confirm your login using an authenticator app on your phone.

When will I be prompted to set up MFA?

- MFA setup does not prompt immediately on your very first sign-in

- You will be prompted to set it up between your 1st and 5th login
- Once prompted, it must be completed to continue using ERMS

Common Questions (FAQs)

1. **Will my old ERMS password still work?**

   No. You must reset your password the first time you log in after the upgrade.

2. **What if my email address has changed?**

   Please contact the Pegasus Health Service Desk so your details can be updated before logging in.

3. **Do I have to use ERMS through a browser?**

   No - ERMS still works via PMS.

   However, your first login and setup is strongly recommended to be completed in a web browser.

4. **How often will I need to use MFA?**

   MFA prompts are managed by Microsoft and may occur:

   - Periodically
   - When logging in from a new device
   - When security risk is detected

Important for shared computers

Logging out of ERMS does not always log you out of Microsoft.

On shared or clinical computers:

- Always sign out of ERMS
- Or use an incognito/private browser

Closing the browser or PMS alone may not log you out.

Need help?

Pegasus Health Service Desk

- Phone: 03 353 9990 (Option 1)
- Email: servicedesk@pegasus.health.nz
- Hours: Monday – Friday | 7:30am – 5:30pm
  (No after-hours support)

Installing an Authenticator App

On iPhone (iOS)

1. Open the **App Store**.

2. Tap **Search** in the bottom-right corner.
3. Type **Microsoft Authenticator** or **Google Authenticator**.
4. Select the app published by
    a. **Microsoft Corporation** (for Microsoft Authenticator) or
    b. **Google LLC** (for Google Authenticator).
5. Tap **Get**, then **Install**.
6. Authenticate with Face ID/Touch ID or your Apple ID password.
7. Once installed, tap **Open** to launch the app.
8. Proceed with instructions of this guide.

On Android:

1. Open the **Google Play Store**.
2. Tap the **search bar** at the top.
3. Type **Microsoft Authenticator** or **Google Authenticator**.
4. Select the app published by
    a. **Microsoft Corporation** – for Microsoft Authenticator
    b. **Google LLC** – for Google Authenticator.
5. Tap **Install**.
6. Once installed, tap **Open**.
7. Proceed with instructions of this guide.