Discovery Health

DISCOVER MORE with HealthID

ACCESSING HEALTHID WITH MULTIFACTOR AUTHENTICATION - FAQS

DISCOVERY HEALTH

Overview

Multifactor authentication is being introduced to enhance the security of HealthID by adding an additional layer of protection to user access.

Multifactor authentication will be activated on HealthID from 15 May 2026.

FAQs

1. What is multifactor authentication (MFA)?

Multifactor authentication is a security measure that requires users to verify their identity using two or more authentication factors when logging in.

In addition to a username and password, users must enter a one-time PIN or password (OTP) sent to their registered cellphone number or email address.

2. Why is multifactor authentication required?

Multifactor authentication significantly strengthens security across Discovery Health digital platforms, including HealthID, the HP Zone and telephonic support channels.

The use of multifactor authentication:

- Protects sensitive healthcare professional, practice and patient information.
- Reduces the risk of unauthorised access.
- Supports compliance with the Protection of Personal Information Act (POPIA) and other regulatory requirements.

To ensure secure access, each individual user within a healthcare practice or bureau must have their own unique login credentials. Shared access and outdated contact details increase security risks and may prevent users from receiving OTPs.

3. What are the benefits of multifactor authentication?

Multifactor authentication provides several key benefits, including:

- Enhanced protection of patient and practice information
- Reduced risk of unauthorised system access
- Stronger overall security posture for healthcare practices and bureau organisations

4. When did Discovery Health start communicating this enhancement?

Discovery Health began communicating the introduction of multifactor authentication in July 2025, when multifactor authentication was first implemented on the Healthcare Professional Zone (HP Zone). At that time, users were informed that multifactor authentication would also be extended to HealthID in future.

In 2026, further communications were issued on 26 March to healthcare professionals, practice personnel and bureau managers, ahead of the 15 May 2026 go-live date. Additional reminders were sent through:

- Pop-up notifications on the HP Zone and HealthID from 27 March 2026
- Interactive voice recording (IVR) messages from 9 April 2026
- Year-end sessions and bureau webinars
- Discovery Health call centre interactions

5. What actions are required from healthcare practices and bureaus?

To ensure uninterrupted access to HealthID once multifactor authentication is live, all users must be correctly registered and linked.

Required steps:

1. Submit the relevant access forms
    - Practice Access Management Form or
    - Bureau Registration and Maintenance Form
2. Ensure personal details are accurate and complete
    - Name and surname
    - ID or passport number
    - Cellphone number
    - Email address

    (These details must match the individual's identification document.)
3. Email completed forms to:
   provider_administration@discovery.co.za
4. Register for a Discovery Digital ID (DDID)
   Once your forms have been processed and acknowledged, you will be invited to register and create your **Discovery Digital ID**. The Discovery Digital ID links the individual user to the relevant practice or bureau and enables access to HealthID and the HP Zone.

How to register for a Discovery Digital ID (DDID)

1. Go to www.discovery.co.za.
2. Click **Register** (top right corner).
3. Select **SA ID number** or **Passport number** and enter the details.
4. Click **Next.**
5. Choose your preferred OTP delivery method (SMS or email) and enter the required details.
6. Enter the OTP received and click **Submit**.
7. Create a username and password.
8. Accept the terms and conditions and click **Register Now.**

Once registered, please ensure that:

- Your preferred OTP delivery method is selected.
- Your contact details remain up to date.

If your contact details change, you may need our assistance to update them.

6. How often will users be required to enter an OTP?

An OTP will be required:

- When logging in from a new device or browser.
- When browser settings (such as cache or cookies) are cleared.
- Once every 90 days per user and per browser, even when using the same device and browser consistently.

This approach ensures both strong security and seamless user experience.

7. Will multifactor authentication be required every time I log in to HealthID?

No. Multifactor authentication will not be required on every login.

Users will only be prompted for an OTP under specific conditions (as outlined above), including the 90-day authentication requirement per user for each browser.

8. What happens if I do not update or verify my contact details before multifactor authentication goes live?

If your contact details are not updated and verified:

- You may not receive your OTP.
- This may result in interrupted access to HealthID.
- You will need to update your details before access can be restored.

9. Can multiple users in a healthcare practice or bureau organisation share one login?

No. Shared logins are not supported under multifactor authentication.

Each user must have:

- Their own unique username and password (DDID).
- Their own registered contact details.

Shared logins may result in access limitations and failed authentication.

10. Can I choose how I receive my OTP?

Yes. Users can select their preferred OTP delivery method:

- SMS to a registered cellphone number.
- Email to a registered email address.

How to do this:

- Contact the Digital Support team on 0860 100 696 to update your OTP settings and confirm your preferred delivery option.
- Alternatively, log in to HealthID and navigate to **Settings** > **Multi-Factor Authentication**.
  Users who have not previously set up their OTP preference can update it here, provided their contact details are already up to date in the system.

11. What should I do if my contact details change?

- You must update your information to maintain access.
- You will need our assistance.
- Keeping your details up to date is essential for receiving OTPs.

How to do this:

- Email provider_administration@discovery.co.za to update contact details (cellphone number and email address) or
- Call the Healthcare Professional (HP) Call Centre to have your details updated.

12. Will multifactor authentication apply to all HealthID users effective 15 May 2026?

Yes. Multifactor authentication applies to all HealthID users, including:

- Healthcare professionals
- Practice personnel
- Bureau personnel

13. Why might I not be receiving my OTP?

Common reasons include:

Scenario	Action
Not registered	Submit registration forms
Shared logins	Register for a unique username and password
Outdated contact details (email or cellphone number)	Update your contact details using available support channels
Poor cellphone network	Contact your service provider
Email delivery delays	Contact your service provider
Do-not-disturb (DND) settings	Disable restrictions
Blocked SMS/email	Check device settings
OTP in spam folder	Check spam or junk folder
Roaming restrictions	Review network settings

14. What happens if I enter the OTP incorrectly?

If the OTP is entered incorrectly:

- You will be prompted to try again.
- Multiple failed attempts may result in temporary access restrictions.

15. How long is an OTP valid?

An OTP is valid for **5 minutes** for security purposes.

If it expires, you will need to request a new OTP.

16. What should I do if I experience ongoing multifactor authentication or login issues?

If you continue to experience issues:

- Confirm your contact details are correct.
- Check your connectivity.
- Ensure SMS or email services are active.

If the issue persists, contact our Digital Support team.

Important notes

- For security reasons, we can only assist users who have been successfully verified.
- OTP settings may only be updated for the verified individual user.
- Shared credentials are not supported and may limit access.

Support options

- **Email**: provider_administration@discovery.co.za to update contact details (cellphone number and email address)
  (Monday to Friday, 07:00 to 16:30)
- **Contact the Digital Support team**: 0860 100 696 to update OTP settings and preferred option
  (Monday to Friday, 07:00 to 18:00)

This is the end of the guide.