Verify Contact Information

Confirm the following information is accurate. Your email or mobile phone number will be used for future logins. If the information is not accurate, press Edit to revise. If no changes are needed, press Continue.

Primary Personal Email
m...r@mail.mil

Primary Personal Phone
...1234

☐ Click here to not show this page again for 1 year.

[Edit] [Continue]

10. Confirm primary email address and primary phone number to make changes. User can also elect to not view this page for one year.

11. Create password.

Must be changed at least every 180 days.

Must be between 15 and 20 characters in length

Must contained 1 uppercase letter, 1 lowercase letter, and 1 number

Special characters are allowed **but** not required.

Password Requirements:

Passwords must be at least 15 characters but no more than 20
✓ At least 1 lowercase letter
✓ At least 1 uppercase letter
✓ At least 1 number
✓ Special characters are optional. Your password can contain these special characters: @,_#&$`%*+0./,=-@!?==<*@-)
✓ No birth dates, Social Security numbers, part of your name, phone numbers, or zip codes.
✓ You cannot change your password more than once every 24 hours.

Enter your password below. Please note that:

1. All passwords expire in 180 days and must be changed prior to expiration. The system will alert you when your password is within 30 days of its expiration date. For your security, do not write your password down.
2. The lines above will turn green as your password meets each of the requirements.
3. You must sign in at least once a year to prevent your account from being deactivated.
4. When finished, always log off and CLOSE all tabs and browser windows to prevent PII loss.

Password 👁 Confirm Password 👁
password is not valid

[Submit] [Cancel]

12. Setup Challenge Questions.

13. Registration Complete.

🔒 DS LOGON | [Log In]

✓ Account Registration
Congratulations! Your username is holly.a.juliett

[Finish]

User must work the steps to setup Multi-Factor Authentication (MFA).

Download "Authy or Microsoft Authenticator".

Open app, create/add account, enter code shown in step 2 to app.

🔒 **DS LOGON**

Verified authentication code [Close]

✓ Verify Two-Factor Authentication

✓ Setup Multi-Factor Authentication

There are apps available to users that will assist in the security of their login information. If you wish to set-up multi-factor authentication, please follow these steps. Otherwise, select Skip below.

Step 1
If you do not already have an authenticator app on your smartphone and you wish to set-up a multi-factor authenticator, you can download Authy or Microsoft Authenticator.

Step 2
In the authenticator app, enter the code as shown. Do not use spaces or dashes.

4BZT HZ4E SAZU I4KN

Step 3
Enter the 6-digit code shown in the authenticator app below.

Authentication code

[Continue] [Skip] [Cancel]

When using an authenticator app, the system will prompt user to enter the 6-digit code from the app as shown. If correct, the system displays confirmation message.

🔒 **DS LOGON** | [Log In]

✓ Verify Two-Factor Authentication

Enter the 6-digit code shown in the authenticator app below.

Authentication code
391492

[Continue]

Verified authentication code [Close]

✓ Authentication

[Continue]

♦ DSL accounts can be locked for a variety of reasons to include unusual activity. Account locks can only be unlocked by DMDC. Account locks are NOT the same as account suspended or an account that has been deactivated.

♦ An account can be suspended due to incorrect password attempts or inactivity.

♦ An account can be removed due to inactivity.

♦ If you have unsuccessfully tried to remote proof multiple times and are now receiving error, your ability to remote proof has been suspended for 30 days. If you try again, the 30 day timelines starts over again. DMDC cannot remove the suspension on your ability to remote proof as it occurs as the data vendor site.

To un-suspend account: Log into DSL, Select Un-suspend My Account, Answer Challenge Questions and Change Password.

NOTE: You MUST complete all the steps at a single time in the time limit of 10 minutes. If you do not complete the process, you timeout, or you provided information that cannot be verified, your ability to access DSL and partner sites may be impacted. Please have documents ready BEFORE you start the process.

Chrome and Edge are recommended browser for optimal user experience.

MHS GENESIS Patient Portal

Activation Guide

https://my.mhsgenesis.health.mil

For customer support, please contact DMDC Customer Contact Center at 800-368-3665.

Go to https://my.mhsgenesis.health.mil

1. Select option "Create Account".

2. Select one of the following options that best describes you.

3. Provide all eligibility information and continue.

4. Click "I agree" to consent to Identity proofing.

5. You must verify your current mailing address.

6. You will receive notification that you've consented to remote proofing.

NOTE: You will remote proof using 1 of 3 random methods.

1st Method: Financial Account & Knowledge-Based Quiz

User must select an account type—credit card or other. When selecting **credit card**, you must enter the **last 8-digits** . When selecting **other account**, the user must enter the **full account number**.

The User must also pass a knowledge-based quiz in less than 3 minutes. The system allows 3 attempts to successfully complete the quiz.

2nd Method: Document Upload

You will have to upload documents for Identity Verification:

- Driver's License
- Border Crossing Card
- Consular ID Card
- Employment Authorization Card
- ID Card
- Passport or Passport Card
- Permanent Resident Card
- State Department ID Card
- Etc.

Take a picture of selected documents and submit for verification. Close page. Click on verification status after waiting 1 minute to monitor status of request.

Will receive notification that upload is complete.

3rd Method: Knowledge-Based Quiz & Document Upload

ONLY 3 attempts to pass the quiz. Must answer within 3 minutes.

Follow 2nd method directions for document upload.

7. Verify contact information.

Verify Two-Multi Factor Authentication (2FA)

8. User will choose phone number to receive one-time -PIN (OTP) and hit "send authentication code".

9. Enter OTP.

Data submitted is only used to verify identity at the time of remote proofing.