

MFA for NHSmail is here!

The purpose of this document is to provide more information about the rollout of Multi-Factor Authentication (MFA) for all NHSmail users and how you as MFA champions can support the implementation of technology enhancements to protect NHS data privacy and patient security.



If you are a Digital Hero, part of the local transformation team within your organisation, or have a lot of familiarity with technology and you are willing to help your colleagues you can **be part of this transformation by becoming an MFA Champion!**

How can you help with the rollout of MFA?

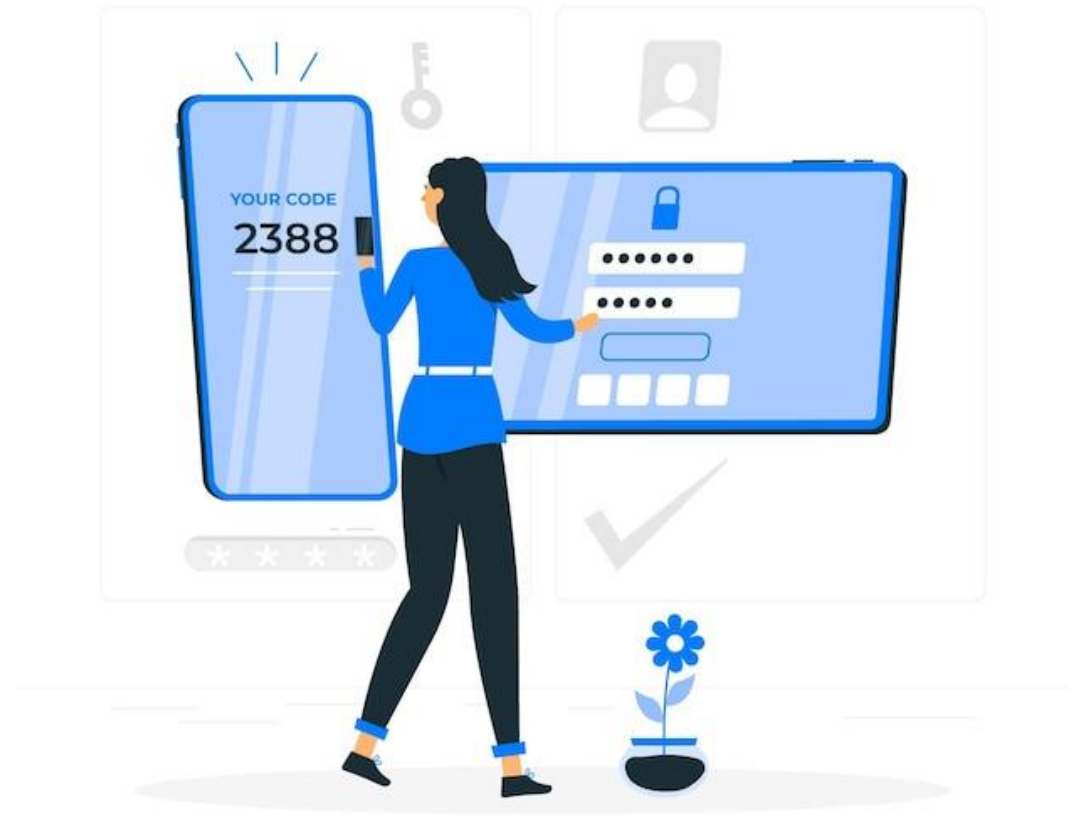
1. Act as the **point of contact** who will help colleagues understand what MFA is and why it is so important
2. Understand how to enrol for MFA and **signpost** your colleagues to relevant guidance and support materials on the [NHSmail Support Site](#)
3. Promote the adoption of MFA by **encouraging** your colleagues to enrol as soon as possible by following the [how-to articles and videos](#) on the NHSmail Support Site

What is MFA?

Multi-factor authentication (MFA) is an additional way of checking that it is really you when you log in to your account.

In addition to your email address and password, you will need to **set up a second form of authentication**, such as an authentication app on your mobile phone, text message or call. This second layer of security is designed to prevent anyone but you from accessing your account, even if they know your password. FIDO2 tokens and NHS smartcards can be used as an additional authentication option to bypass MFA prompts once a core MFA method (authentication app, text or call) has been set up on the account.

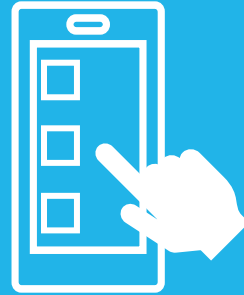
The rollout of MFA will help NHSmail meet industry and cyber security best practice, helping to **protect NHS data, user personal data and patient data**.



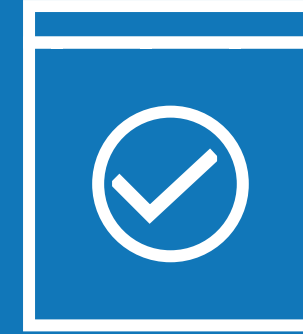
Multi-Factor Authentication



Password



Verification



Access

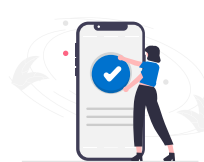
Why is MFA important to the NHS?



Keeps any **patient data** in a more protected environment



Helps you gain access to your account should you **forget your password**



Helps protect **NHS reputation**



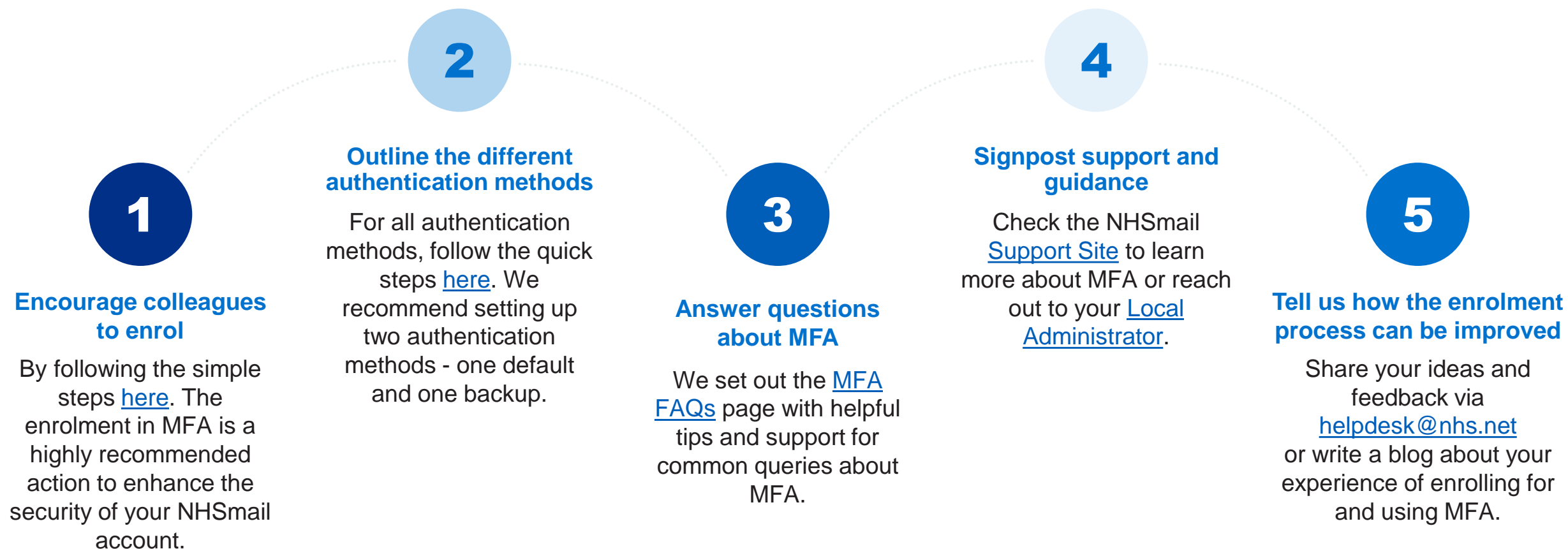
Provides increased protection **against cyber attacks**



Checks if an attempt is made to access your account from an **unusual location** or device

How do we get started with MFA?

As the point of contact for MFA, you will promote enrolment and support colleagues through the process.



What options do we have to enrol?

The recommended authentication method is the Microsoft Authenticator app on your Android or iOS mobile device. Once these methods are set up, FIDO2 tokens and NHS Smartcards can be used to bypass prompts.



Authenticator App

Download the Microsoft Authenticator app on your smartphone to verify your sign in or to get a verification code.

[FIND OUT MORE](#)



Text message

A text message (SMS) is sent to the mobile phone number registered containing a verification code.

[FIND OUT MORE](#)



Phone Call

An automated voice call is made to the mobile phone number registered prompting the user to press # on their keypad.

[FIND OUT MORE](#)



FIDO2 Token

Use FIDO2 to bypass MFA prompts and sign in with a choice of security keys available and supported.

[FIND OUT MORE](#)



NHS Smartcard

If you have a Care Identity Smartcard, register it in “My Identity Portal” and use it to access NHSmail and Office 365 applications.

[FIND OUT MORE](#)

Clarifying facts about MFA...

MYTHS

FACTS

MFA is difficult to set up and use.



MFA is quick and easy for most people to set up and you can select the authentication method that best suits your needs.

I do not need MFA because my account has never been compromised.



No matter how strong your password is, there is always the threat of a cyber-attack. MFA is important because it makes it harder for hackers to steal your information.

I only have one option for authenticating my log in.



There are three authentication methods you can choose from: Microsoft Authenticator app, text message or phone call. FIDO2 token and NHS smartcard are additional authentication methods.

I need an internet connection to use the Microsoft Authenticator app.



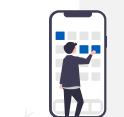
You need an internet connection to receive a push notification on the Microsoft Authenticator app but not to access a one-time passcode.

The Microsoft Authenticator app will collect my personal data.



The Microsoft Authenticator app does not collect or store any personally identifiable data. Your personal mobile device details are not used for any purpose other than protecting your account.

I do not need to enable MFA via mobile app, text or call if I use an NHS Smartcard or FIDO2 token.



You should enable MFA using mobile app, text or phone call in addition to using an NHS Smartcard or FIDO2 token.



What should I do if I need help?

1. Check the Support Site articles [here](#)
2. Reach out to your [Local Administrator](#)
3. Contact the NHSmail Helpdesk by calling 0333 200 1133 or emailing helpdesk@nhs.net

For feedback, please contact us via [Your Voice](#)

Thank you for
becoming an
MFA Champion!

