Department of Health & Social Care

NHS England

Classification: Official

To:
- All NHS trusts:
  - chief executive officers
  - chief information officers
  - chairs
- ICB:
  - chief executive officers
  - chief information officers
  - chairs
- Arm's length bodies
  - chairs

NHS England
Wellington House
133-155 Waterloo Road
London
SE1 8UG

29 February 2024

Dear colleagues,

Multi-factor authentication

Ensuring good cyber security is essential to safeguarding health and care services; our Cyber Security Strategy for Health and Social Care looks to build a more cyber secure heath and care service for the future. In an increasingly digitised service, organisational leaders are accountable for managing their own organisational cyber risk, to protect valuable data and build patient and service user trust in our systems.

Multi-factor authentication (MFA) is widely recognised as one of the most effective ways to protect data and accounts from unauthorised access, preventing 99.9% of account compromise attacks.

When enabled, MFA requires users accessing systems to present proof of at least two factors from:

- something they know (such as a password)
- something they have (such as a device)
- something they are (biometrics, like a fingerprint or iris scan)

This extra layer of security means our systems are far less likely to be attacked, and our data and ability to continue to provide patient care is much more secure. Its use in the NHS will help protect patient data and organisations' capability to deliver patient care.

Key dates

We are writing to remind you of the key dates for the implementation of MFA as a critical cyber security measure:

- Thursday 29 February 2024: interim 2023-24 Data Security and Protection Toolkit submissions, which should include your progress towards implementation on all systems
- Sunday 30 June 2024: final Data Security and Protection Toolkit submissions, which should include your confirmation of full implementation on all systems
- Sunday 30 June 2024: NHSmail enable MFA for all NHSmail user accounts

These dates are in line with our recently published MFA Policy for the NHS, which will ensure that MFA is used on digital systems throughout the health sector, with particular requirements on accounts that are remotely accessible or have privileged access to systems.

What you need to do

The actions described below were published as part of the enforcement intent for the national MFA policy. For the avoidance of doubt, we are asking: chief information officers to ensure these actions are completed; chief executive officers to support them; and boards to assure themselves that actions are taken and monitored.

By **29 February 2024**, organisations are expected to provide the National Chief Information Security Officer [CISO] (using their interim submission of the 2023-24 Data Security and Protection Toolkit) with **either**:

- confirmation of full compliance with the MFA policy
- confirmation that plans are in place to achieve full compliance by June 2024, and a summary of the plans

By **30 June 2024**, organisations are expected to provide the National CISO (using their final submission of the 2023-24 Data Security and Protection Toolkit) with **both**:

- confirmation of full compliance with the MFA policy, with MFA implemented on all relevant systems
- details of exceptions, as required by the policy

The Department of Health and Social Care expects to use its enforcement powers under the Network and Information Systems (NIS) Regulations where insufficient assurance is provided at the second checkpoint.

Further support

If you would like a briefing or conversation with national teams about this advice and the importance of MFA and the risks it mitigates, please do contact us at england.cyber@nhs.net.

Yours sincerely,

Phil Huggins
National Chief Information Security Officer
Department of Health and Social Care

John Quinn
Chief Information Officer
NHS England