RSA | BlueFort Security

SOLUTION BRIEF

Health Check: The modern MFA capabilities NHS organisations must prioritise to meet the new NHS England requirements

Securing access to sensitive data, assets, and resources with multi-factor authentication (MFA) is a core cyber security component. And because MFA has proven to be so effective, NHS England announced new cyber security requirements mandating NHS trusts, integrated care boards, arm's length bodies of the Department of Health and Social Care, and other healthcare providers must demonstrate plans to implement MFA by February 2024 and achieve full compliance by the end of June 2024.

To comply with the MFA requirement, NHS organisations must understand the identities their organisations manage and the services and privileges required by disperate user groups. They also need to consider how to effectively balance security and convenience. Finally, they must ensure that certain systems and services remain operational.

So let's detail the capabilities that NHS Trusts should prioritise to achieve the MFA requirements and keep patients, medical staff, and their families healthy, happy, connected, and secure.

Secure multiple environments

As a minimum, NHS organisations must have MFA "enforced on all remote user access to all systems" and ensure MFA is "enforced on all privileged user access to externally-hosted systems."

In addition to this requirement, NHS organisations should thoroughly review their identity security posture as a whole and extend new security capabilities to as many users as possible. Similarly, they should assess how they're protecting Service Accounts and non-human entities on the network – all of which can increase the attack surface and may not receive the same degree of scrutiny as human actors.

NHS organisations should ensure that their MFA solution is adaptive or elastic enough to meet its needs as an organisation: the solution should be available in the cloud, hybrid deployments, and on-premise. Moreover, it should seamlessly flex between environments without disrupting services or requiring re-engineered resources. Ultimately, the solution should be able to secure the organisation's environment today and be adaptive enough to secure additional environments in the future, particularly if NHS organisations move resources to the cloud.

Provide expansive user choice

MFA solutions should cater to user choice and allow for various MFA options to meet all user needs. RSA provides a vast number of ways to authenticate; Biometric, push to approve, smart card, FIDO token, hardware tokens, wearables, to name a few. This encourages broader adoption by allowing users to leverage the most suitable authentication type available.

Cyber attacks target NHS

Threat actors are targeting the NHS' digital systems:

- **September 2023:** The NCSC noted state-sponsored actors "targeted…the NHS during the height of the pandemic"
- **July 2023:** The BlackCat Ransomware syndicate stole 7TB of patient data from Barts Healthcare NHS Trust
- **June 2023:** Millions of NHS medical devices revealed to be unprotected from threat actors
- **August 2022:** NHS IT provider Advanced hit by a ransomware attack

OWN YOUR IDENTITY.

Balance security and convenience

NHS Trusts should also prioritise capabilities that balance security and convenience. They can find that balance by leveraging one of the market's most mature risk and identity assurance engines: RSA Risk AI allows organisations to baseline user behaviour and automate challenges only when needed. The system dynamically assesses access rights, job roles, application usage and a number of other factors to ascertain whether a user should be granted access, challenged, or denied access.

Focus on resources as well as users

In addition to protecting users, NHS Trusts should also consider how they protect their APIs and other third-party resources. NHS Trusts should use integrations built on open standards: RSA supports a range of integrations with the vast majority of applications without requiring the use of agents. Having authentication capabilities that can extend across all resources enables IT teams to confidently assure the business that all resources are protected at all times and provide users with a seamless experience.

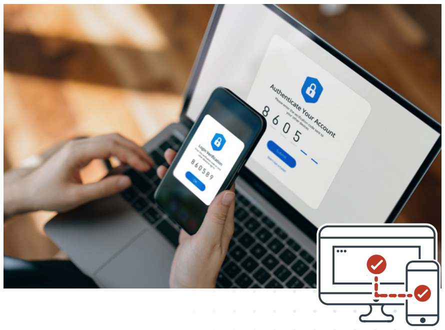
Keep patients connected, healthy, and secure

Implementing MFA is a critical component of a broader identity and access management (IAM) strategy, and the new NHS England MFA requirement provides NHS organisations with a valuable opportunity to review their strategies.

That review should include assessing the organisation's existing directories (Active Directory, Entra AD etc.) and consolidating what may be disparate systems into a single, unified identity solution.

With nation-state attacks and ransomware syndicates targeting healthcare providers, the NHS MFA mandate allow NHS organisations to address critical cyber security risks. To fulfill the requirements, fortify their cyber security posture, and gain additional value from their MFA solution, NHS organisations should work with trusted advisors like BlueFort and RSA to:

- Identify all their applications, programming interfaces, and resources
- Develop an MFA strategy that protects all resources, regardless of the type, age, location, or protocol needed for authentication
- Provide a consistent, seamless, and frictionless experience for end users either in the cloud, across hybrid environments, or on premise



NHS England MFA mandate Timeline

- **August 2023:** The Data Alliance Partnership Board updates section 250 of the Health and Social Care Act of 2012; this newest revision requires NHS bodies to "make specific improvements on MFA"
- **February 2024:** Deadline to demonstrate implementation plans
- **June 2024:** Full policy compliance
- **June 2025:** Post Implementation review

About BlueFort

BlueFort is the UK's leading Independent Security Solutions Partner (SSP) providing a unique combination of people and technology focused on simplifying your cyber journey. With a curated suite of tools, products and skills, BlueFort partners with CISOs and SecOps teams to simplify, consolidate, optimise and transform their cyber security environment. BlueFort's carefully tested suite of tools and technology simplifies the chaos of the cyber landscape, while its in-house experts provide a rapid and immediate solution to the cyber security skills shortage, reducing pressure on internal security teams.

About RSA

The AI-powered RSA Unified Identity Platform protects the world's most secure organisations from today's and tomorrow's highest-risk cyberattacks. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. More than 9,000 security-first organisations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For more information, go to RSA.com.