

Multi-Factor Authentication Policy V1.0

Cornwall Partnership NHS Foundation Trust document reference code: IT/018/25

Purpose: This policy sets out the requirements for the use of Multi-Factor Authentication as a cyber security control to establish a consistent minimum expectation. The requirements of this policy are incorporated into the mandated principles of the Data Security and Protection Toolkit (DSPT, CAF-DSPT, DSP Toolkit). The objective of this policy is to promote and ensure the widespread use of MFA as a fundamental cyber security control, in order to manage the data security risks associated with user credential compromise.

Target audience: This policy applies to all staff members of the Cornwall and Isles of Scilly ICS member organisations, the Cornwall and Isles of Scilly ICS members.

Document Sponsor and role: Martin Price, Cyber Security Lead

Document Sponsors contact details: 01872 250000

Document definition: Policy

Audience:

- ☒ Royal Cornwall Hospitals NHS Trust
- ☒ Cornwall Partnership NHS Foundation Trust

Freedom of information: Can be released under the Freedom of Information Act 2000. This document will be published on the internet and intranet.

Key words: Authentication, login, admin, administrator, privileged, root, superuser

Royal Cornwall Hospitals NHS Trust approval process

General manager confirming approval processes: Chief Information Officer.

Governance lead confirming approval process: Mark Scallan.

Supporting committee: Information Governance Committee.

Supporting chairperson: Alison Thorne-Henderson, Chief People Officer

Executive director responsible for the policy: Chief Information Officer.

Approved at: Information Governance Group.

Date approved: 14 October 2025

Executive approval: Kelvyn Hipperson, Chief Information Officer.

Date approved by: 14 October 2025

Approved at: Royal Cornwall Hospitals NHS Trust Policy Ratification Group

Date approved: 19 November 2025

Document library folder and sub-folder: Health Informatics / Infrastructure - Technical - Security

Cornwall Partnership NHS Foundation Trust approval process

Accountable Executive: Chief Information Officer

Supporting committee: Information Governance Sub-Committee

Supporting chairperson: Sarah James, Chief Improvement Officer

Approved at (if applicable): Information Governance Sub-Committee

Date: 26 September 2025

Accountable Executive approved: Chief Information Officer

Date: 8 December 2025

Document library section: Information management and IT, Information technology.

Ratification

Start date: 8 December 2025

Review date: 8 June 2028 (6 months prior to the expiry date).

Expiry date: 8 December 2028 (3 years after ratification unless there are any changes in legislation or changes in NICE guidance or national standards).

Version control summary

Version	Date	Sponsor and/or reviewer	Changes (key points)
V1.0	April 2024	M. Price, Cyber Security Lead	V1.0 created

Contents

1. Introduction.....	7
2. Scope	7
3. Definitions and glossary	8
4. Ownership and responsibilities	10
4.1. Role of the Chief Information Officer	10
4.2. Role of the Senior Information Risk Owner	10
4.3. Role of the Information Governance Group/Sub Committee/Steering Group.....	10
4.4. Role of the Information Asset Owners.....	10
4.5. Role of the Line Managers	10
4.6. Role of Cornwall IT Services	11
4.7. Role of Individual Staff	11
5. Standards and practice	11
5.1. Remote User Access to all Systems	11
5.2. Privileged User Access to Externally Hosted Systems.....	11
5.3. Privileged User Access to all Other Systems	11
5.4. Exceptions.....	11
5.4.1. General Exceptions.....	11
5.4.2. Specific Exceptions	12
5.5. Authentication Factors.....	12
5.6. Selecting Authentication Factors	13
5.7. Personal Devices	13
5.8. Federated Authentication	13
5.9. Resilience and Recovery.....	13
6. Related legislation, national and local guidance	14
7. Implementation.....	14
8. Document monitoring arrangements	15
9. Environmental sustainability	15
10. Updating and review	15
11. Equality and diversity	16
Appendix 1: Equality Impact Assessment Form	17
Appendix 2: General Exceptions	19
Appendix 3: Specific Exceptions.....	20

Appendix 4: Authentication Factors 21

Data Protection Act 2018 (UK General Data Protection Regulation Legislation)

The Trusts have a duty under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 to ensure that there is a valid legal basis to process personal and sensitive data. The legal basis for processing must be identified and documented before the processing begins. In many cases we may need consent, this must be explicit, informed, and documented. We cannot rely on opt out; it must be opted in.

Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 is applicable to all staff; this includes those working as contractors and providers of services.

For more information about your obligations under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679, contact the Information Governance team.

- Cornwall Partnership NHS Foundation Trust: Email cpn-tr.infogov@nhs.net
- Royal Cornwall Hospitals NHS Trust: Email rch-tr.infogov@nhs.net

1. Introduction

- 1.1. Compromising user accounts is a starting point for many cyber security attacks.
- 1.2. Common or easily guessed passwords can be breached with unsophisticated attacks, giving attackers easy access to an organisation's systems and enabling them to deploy ransomware.
- 1.3. Many people use the same or similar passwords in multiple systems, making a compromise potentially more damaging.
- 1.4. Users typically authenticate to systems by presenting either something they know (such a password), something they have (usually a device), or something they are (biometrics). Multi-factor authentication (MFA), the use of two or more of these authentication factors, is an effective control against a wide range of account compromise techniques, stopping simple attacks altogether and making it sufficiently more difficult for sophisticated attacks to succeed.
- 1.5. This version supersedes any previous versions of this document.

2. Scope

- 2.1. The responsibilities, standards and practice described in this policy must be applied to:
 - All access to CITS provided systems by staff members using remote access.
 - All privileged access by staff members to externally hosted systems.
- 2.2. It is recommended that the responsibilities, standards and practice contained in this policy be applied to:
 - All privileged user access to all other systems.
- 2.3. This policy applies to, but is not limited to employees, non-executive directors, contractors, agency staff members, researchers, trainees, students and volunteers.
- 2.4. It describes the responsibilities about the use of MFA whilst accessing systems hosted by CITS or authorised for use by a Cornwall and Isles of Scilly ICS member organisation.

- 2.5. A failure to follow the requirements of this policy may result in investigation and management action being taken as considered appropriate. This may include formal action in line with the organisation's disciplinary or capability procedures for employees or action, in relation to other staff members, that may result in the termination of a contract, assignment, placement, secondment or honorary arrangement.
- 2.6. Non-compliance may also lead to civil or criminal action being taken.

3. Definitions and glossary

- 3.1. **Authentication** - the process of verifying the identity of a user attempting to gain access to a system.
- 3.2. **Cornwall and Isles of Scilly Integrated Care System**: Made up of the Cornwall and Isles of Scilly Integrated Care Board, the Royal Cornwall Hospitals NHS Trust, the Cornwall Partnership NHS Foundation Trust, Kernow Health and the GP practices across Cornwall and the Isles of Scilly, collectively the Cornwall and Isles of Scilly ICS member organisations, the Cornwall and Isles of Scilly ICS members.
- 3.3. **Cloud / Cloud computing**: Typically, web-based technology that allows users to access and utilise computing resources over the internet, rather than relying on on-premises systems.
- 3.4. **Cornwall CoIN**: A CITS managed Community of Interest Network (CoIN). This wide area network links all the computers across all Cornwall and Isles of Scilly ICS member organisations sites with the national HSCN network.
- 3.5. **Credentials**: Information that helps identify, validate and define users and their access privileges, typically a username and password.
- 3.6. **Data Security and Protection Toolkit**: The DSPT, CAF-DSPT, DSP Toolkit. An online system which allows organisations to assess themselves or be assessed against NHS England Information Governance and Data Protection policies and standards.
- 3.7. **Externally hosted**: Applications, IT infrastructure components or functions that organisations access from external service providers, usually through an internet connection. Cloud computing is typically externally hosted.
- 3.8. **Federated Authentication**: A means of providing user authentication and identity verification to various systems using only one set of credentials.

- 3.9. **Health and Social Care Network (HSCN):** A data network for health and care organisations that provides the underlying network arrangements to help organisations access systems easily and smoothly and share information more reliably, flexibly and efficiently.
- 3.10. **Information Asset Owner:** Usually, a senior member of staff who is the nominated owner for one or more identified information assets (e.g. database or IT system) of the organisation and is responsible for the identified information asset.
- 3.11. **Multi-Factor Authentication (MFA):** an electronic authentication method in which a user is granted access to a system only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.
- 3.12. **Must:** This word, or the terms “required” or “shall”, mean that the definition is an absolute requirement of this policy.
- 3.13. **Personal Identifiable Data (PID):** Any information that is personal to an individual and would identify a person as that individual, e.g. name, NHS number.
- 3.14. **Privileged User:** A user that is authorised (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorised to perform.
- 3.15. **Remote Access:** The ability to access information stored on the Cornwall NHS Network from a device not directly connected to it.
- 3.16. **Service Account:** A user account that is created explicitly to provide a security context for services, typically found on Windows Server operating systems.
- 3.17. **Should:** This word, or the adjective “**recommended**” mean that there may be valid reasons for not applying the requirement, but the full implications must be understood and carefully considered.
- 3.18. **Social Engineering:** A manipulation technique that exploits human error to gain private information or access to systems.
- 3.19. **System:** Applications, IT infrastructure components or functions that organisations access internally, usually through a connection to the Cornwall CoIN or via remote access.
- 3.20. **User:** Any individual (other than a patient or person in care) or system process authorised to access an information system and, therefore, includes service accounts.

4. Ownership and responsibilities

4.1. Role of the Chief Information Officer

The Chief Information Officer (CIO) has overall accountability for the implementation of MFA across the Cornwall and Isles of Scilly ICS and for ensuring its continued use.

4.2. Role of the Senior Information Risk Owner

The SIRO has accountability for ensuring that effective systems and processes are in place to manage the risks relating to the use of multi-factor authentication, retains overall accountability for information governance and is the overall owner of information risk within the organisation.

4.3. Role of the Information Governance Group/Sub Committee/Steering Group

The organisation's Information Governance Group/Sub Committee/Steering Group, herein known as the Information Governance Group, is responsible for:

- Ratifying the policy.
- Ensuring that it is disseminated to all relevant staff members.
- Approve all exceptions as defined by this policy and undertake an annual review of these exceptions.

4.4. Role of the Information Asset Owners

Information Asset Owners are responsible for:

- Ensuring that the requirements for privileged access for users of any externally hosted IT systems that they are responsible for have been identified.

4.5. Role of the Line Managers

Line managers are responsible for:

- Reinforcing the staff member's responsibility for confidentiality and security of data and the need for MFA.

4.6. Role of Cornwall IT Services

CITS are responsible for:

- Implementing MFA in accordance with good practice guidance.
- Understanding, documenting and risk-assessing all exceptions as defined in this policy.

4.7. Role of Individual Staff

All staff members are responsible for:

- Ensuring that they have read and understood this policy.
- Ensuring that any usage of MFA conforms to IT policies, NHS standards and UK legislation.
- Learning how to use MFA solutions and how to authenticate safely and appropriately.

5. Standards and practice

5.1. Remote User Access to all Systems

All access to systems by staff members using remote access must have MFA enforced unless one of the permitted exceptions, described in later sections apply.

5.2. Privileged User Access to Externally Hosted Systems

All privileged user access to externally hosted systems must have MFA enforced unless a permitted exception applies.

5.3. Privileged User Access to all Other Systems

MFA should be enforced on all privileged user access to all other systems other than when a permitted exception applies.

5.4. Exceptions

Exceptions are provided to allow the Cornwall and Isles of Scilly ICS member organisation, the organisation, to balance clinical and operational requirements with cyber security risk.

5.4.1. General Exceptions

5.4.1.1. General exceptions may be used without needing to report or justify the reliance. However, the risk that is created by reliance on potentially wide-ranging exceptions must be understood. The use of MFA as an appropriate control in such scenarios, such as those involving approving large payments, for example, should be considered.

5.4.1.2. The table in Appendix 2 provides a list of the current general exceptions.

5.4.2. Specific Exceptions

5.4.2.1. Specific exceptions should only be used when necessary and the organisation must:

- Understand, document, risk-assess and internally approve all exceptions.
- Ensure that an annual review is conducted of all specific exceptions to confirm that they are still relevant and appropriate.

5.4.2.2. The organisation must use caution when applying specific exceptions, especially in situations where the implementation of MFA would create disproportionate clinical or operational risk. There should be demonstrable evidence that the cyber risk of not enforcing MFA has been compared against the clinical or operational risk of enforcing MFA and that alternative controls and mitigation measures have been considered.

5.4.2.3. The table in Appendix 3 provides a list of the current specific exceptions.

5.5. Authentication Factors

5.5.1. The organisation is not constrained to a specific technical approach to MFA unless specifically mandated or prohibited by NHS England, although the risks of the selection of an authentication factor should be documented and assessed and accepted at the appropriate level. Potential controls to mitigate the identified risk and periodically review the suitability and effectiveness of the authentication factor should be carefully considered.

5.5.2. It should be recognised that some authentication factors, such as biometric factors are stronger than, for example, SMS text messages. The risks of using authentication factors that are considered weaker should be carefully

considered, particularly with IT systems that provide access to personal identifiable data or sensitive information.

- 5.5.3. The table in Appendix 4 provides a list of authentication factors and their strengths.

5.6. Selecting Authentication Factors

- 5.6.1. A second 'knowledge' requirement, such as the answer to a security question, must not be treated as an additional authentication factor, except for one-time passwords or MFA recovery codes.
- 5.6.2. The data protection obligations must be considered by the organisation before using an MFA solution that collects or processes PID, such as personal contact details or biometric information.

5.7. Personal Devices

There should not be an expectation for staff members to own or use a personal mobile device for work purposes, or to disclose personal contact information to the organisation for the purpose of MFA, although it should be borne in mind that access to digital systems may be limited if a suitable MFA solution cannot be found.

5.8. Federated Authentication

Federated authentication using, for example, NHSmail or NHS Care Identity Service 2, may be implemented by the organisation to provide MFA for a system, particularly for systems that do not otherwise support MFA.

5.9. Resilience and Recovery

- 5.9.1. The organisation should consider the resilience of the authentication factors chosen and options available to staff members should they have lost authentication token.
- 5.9.2. Consideration should be given to the configuration of additional authentication factors to be used when the primary authentication factor is not available.
- 5.9.3. The risk of MFA being breached, particularly using social engineering, should be understood, documented and risk assessed.

6. Related legislation, national and local guidance

6.1. Links to key external standards:

- NHS England multi-factor authentication (MFA) policy (August 2023).
- Data Protection Act 2018.
- Human Rights Act 1998.
- Computer Misuse Act 1990.
- Confidentiality: NHS Code of Practice (November 2023).
- Caldicott Principles (December 2020).
- NHSmail Access Policy (August 2021).
- NHSmail Acceptable Use Policy (November 2023).
- Data Retention and Information Management Policy (December 2022).

6.2. Related documents:

- IT Security Policy.
- Acceptable Use Policy.
- Email Policy.

7. Implementation

- 7.1. This policy should be made available and referenced as part of the implementation of new systems.
- 7.2. Line managers have a responsibility to ensure that their staff, that use MFA, understand and comply with this policy.
- 7.3. This policy will be published on the Document Library.

8. Document monitoring arrangements

Information category	Detail of process and methodology for monitoring compliance
Element to be monitored	This policy will be monitored to ensure that the Cornwall and Isles of Scilly ICS are compliant with the Data Security and Protection Toolkit.
Lead role	Cyber Security Operations Centre Manager.
Tool	The Data Security and Protection Toolkit submission will be used to monitor that the Cornwall and Isles of Scilly ICS are compliant with the Toolkit.
Frequency	Annual.
Reporting arrangements	Incidents or breaches of this policy are reported to the Chief Information Officer, which may also be reported to the Cornwall Cyber Reference Group depending on their seriousness.
Acting on recommendations and lead(s)	CITS Cyber Security Operations Centre.
Change in practice and lessons to be shared	Required changes to practice will be identified following changes in national policy, Data Security and Protection Toolkit requirements and as a result of any Toolkit submissions.

Will the monitoring arrangements result in a clinical audit: No

9. Environmental sustainability

The Trusts are committed and obligated to reduce their environmental impacts. Healthier outcomes can be achieved for people, the planet and pounds by conducting our activities in a more environmentally sustainable manner.

10. Updating and review

10.1. This policy will be reviewed no later than every three years.

10.2. Revisions can be made ahead of the review date when the procedural document requires updating. Where the revisions are significant and the overall policy is changed, the CITS Cyber Security Operations Centre will resubmit the policy to the organisation's Information Governance Group for consultation, ratification and dissemination.

- 10.3. Any revision activity will be recorded in the Version Control Table as part of the document control process.

11. Equality and diversity

This document complies with the Cornwall Partnership NHS Foundation Trust and Royal Cornwall Hospitals NHS Trust equality and diversity statements. The statements can be found in the [RCHT Equality Diversity And Inclusion Policy](#) and [CFT Equality, Diversity and Inclusion Statement](#).

The initial equality impact assessment screening form is at appendix 1.

Appendix 1: Equality Impact Assessment Form

Title of policy or document for assessment: Multi-Factor Authentication Policy V1.0.

Document library section: Cornwall IT Services.

Is this a new or existing document? New.

Date of assessment: 4 April 2025.

Person responsible for the assessment: Martin Price, Cyber Security Lead.

What is the main purpose of the document?

This policy sets out requirements for the use of MFA as a cyber security control to establish a consistent minimum expectation.

Who is affected by the document?

☒ Staff ☐ Patients ☐ Visitors ☐ Carers ☐ Other ☐ All

The document aims to improve access, experience and outcomes for all groups protected by the Equality Act 2010.

Concerns

Are there concerns that the procedural document could have a differential impact on the following areas?

If a negative impact has been identified, please complete a full EIA by contacting the Equality, Diversity, and Inclusion Team. For Royal Cornwall Hospitals NHS Trust please contact rcht.inclusion@nhs.net and for Cornwall Partnership NHS Foundation Trust please contact cft.inclusion@nhs.net

Concern area	Response	If yes, what existing evidence (either presumed or otherwise) do you have for this?
Age	☐ Yes ☒ No	
Disability	☐ Yes ☒ No	
Sex	☐ Yes ☒ No	
Gender reassignment	☐ Yes ☒ No	
Pregnancy and maternity	☐ Yes ☒ No	
Race	☐ Yes ☒ No	
Religion and belief	☐ Yes ☒ No	
Sexual orientation	☐ Yes ☒ No	

Concern area	Response	If yes, what existing evidence (either presumed or otherwise) do you have for this?
Marriage and civil partnership	☐ Yes ☒ No	
Groups at risk of stigma or social exclusion such as offenders or homeless people	☐ Yes ☒ No	
Human rights	☐ Yes ☒ No	

Are there any associated objectives of the document? If yes, what existing evidence (either presumed or otherwise) do you have for this?

No.

Signature of person completing the equality impact assessment:

Name: Martin Price, Cyber Security Lead.

Date: 4 April 2025.

Appendix 2: General Exceptions

No.	Exception	Comments
1.	Unprivileged user account access from within the organisation's trusted corporate network	MFA is required for all user access originating outside the trusted corporate network
2.	Access to a system to which the same user has previously authenticated with MFA from the same device	MFA enforced on first access; user may then subsequently access the same system from the same device without MFA, for an organisation-defined period of time (session management)
3.	Accounts used solely by patients or people in care	Not in scope of this policy. DCB3051 establishes standards for identify verification and authentication for patients and service users

Appendix 3: Specific Exceptions

No.	Exception	Comments
1.	Accounts used by staff with disabilities that make MFA unusable	Consider disabilities equality as part of implementation planning and choice of factors
2.	Access from specific trusted physical locations	Such as access from prisons and other sites with specific restrictions and compensating controls
3.	Systems that cannot support any form of MFA	Federated authentication with an MFA-capable system is considered 'supporting MFA'
4.	Situations in which MFA would create disproportionate clinical or operational risk or difficulty	Organisations must consider alternative controls and mitigations for the security risk

Appendix 4: Authentication Factors

Strength	Authentication Factor	Comments
Basic	SMS text message or voice message to trusted number.	Should not be used unless no better alternative is available, due to susceptibility to unsophisticated attacks.
Better	Mobile push notification.	Number matching or equivalent two-way verification improves attack resistance.
	One-time password (OTP) generated by application or hardware token.	Time-based one-time passcode (TOTP) is more resistant to attack than HMAC-based, Hash-based Message Authentication Code, passcode (HOTP).
	Trusted end user device proved by a device certificate or similar.	Non-exportable credentials are preferable.
Best	Public key infrastructure (PKI), such as NHS Care Identity Service smartcard.	Phishing-resistant.
	FIDO / WebAuthn or U2F.	