NHS England

Data Security Standard 4

Managing data access

The bigger picture and how the standard fits in

2023/24

Information and technology for better health and care

Contents

Overview

The National Data Guardian (NDG) review's data standard 4 states that:

"Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals."

The principle of 'least privilege' is applied, so that users do not have access to data they have no business need to see. Staff do not accumulate system accesses over time. User privileges are proactively managed so that there is, as far as is practicable, a forensic trail back to a specific user or user group. Where necessary, organisations will look to non-technical means of recording IT usage (such as sign in sheets, CCTV, correlation with other systems and shift rosters).

Please refer to further note on professional judgement, auditing and UK General Data Protection Regulation (UK GDPR).

https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/using-professional-judgement

Systems holding personal confidential information - Part 1 (4.1.1 - 4.2.4)

Definitions and scope from National Data Guardian report

Personal data, in the context of health and care, is confidential information that is held (in paper format in some instances, but increasingly digitally) about staff and patients / service users.

This type of information would be held in systems such as:

- electronic patient record systems (EPR)
- picture archiving and communication systems (PACS)
- digital social care record
- patient administration systems
- staff rostering systems
- payroll
- data warehouses
- a clinical correspondence system

Know your staff

Your organisation should keep a staff repository (normally within a HR department) of current staff and their roles. This repository should be up to date and reflect when staff are recruited, their change of roles and if they have left the organisation. Typically, in NHS organisations, this information can be found in the ESR (Electronic Staff Record).

One of the biggest challenges for any organisation is tracking role changes of staff, especially when they remain on the same grade or have multiple roles.

Your organisation can strengthen its approach by implementing and monitoring a strong joiners, movers and leavers policy.

Know your systems

Your organisation should keep a register of all its systems. This encompasses systems that hold personal data, and those that do not, such as those holding corporate information.

Access to systems

There should be access controls within your organisation's systems, and staff members should understand how and why these have been applied. Access to the system might be managed by the system itself, such as where you will enter your username and password, biometrics (fingerprint or facial) or insert a Smartcard to gain access to that system, or alternatively a form of federated access might be used in which a single account is trusted across multiple IT systems, as is the case with Single Sign On (SSO).

Regardless of how this is managed, you should know who has access to the information within systems, with this responsibility normally falling to the Information Asset Owner (IAO). If that information is shared with another system (such as through interfacing), you should know who has access to that system too. This Data Security Standard is not interested in how access works (such as username and password, smartcard or biometric), but uniquely who has access to the information in the systems.

Individual logins are important to use so that you can detect inappropriate access and apply specific access restrictions where needed. If a system does not have the capability for individual logins or they are not used for another reason, you must have a way of managing who has access to the system, and you must consider the mitigations for the associated risks.

Role-based access controls

One of the principles of data protection law is that you ensure that the data you use is adequate, relevant and the minimum necessary for your purpose. This ensures that confidentiality is maintained as access is granted on a need to know basis, whilst ensuring that staff have access to the data needed for their role.

Role-based access controls are key to achieving these requirements. You should ensure that all staff members are granted exactly the right level of access to fulfil their roles.

For each of your systems that have role-based access controls applied, you should list the type of role (such as admin) and the number of users who have been set up with that type of account.

A simple example is given below:

Simple sample system		
Role	***Description***	***Number of accounts***
Admin	Ability to amend, delete and create new tables and look up fields	2
General user	Ability to add, amend and delete own created records and view others	50
Super user	Ability to add, amend and delete own created records, amend and view others	3
View user	Ability to view all records	8
Backup user	Technical account used to archive the systems database	1

‘Least privilege’ should be at the centre of who has access to which roles. Referring to the table above, if a user only needs to view records, there is no need for them to have an elevated role such as ‘admin’ or ‘super user’. The ‘view user’ role will give them the level of access they require.

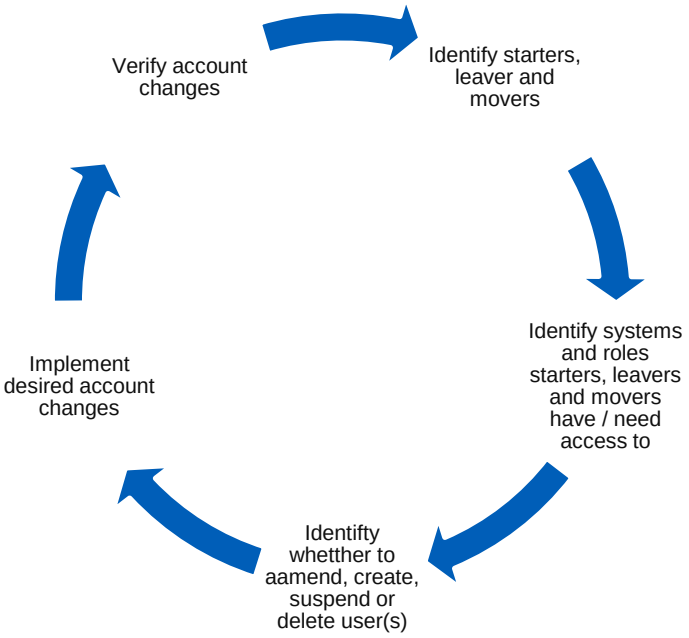
As organisations become larger, it can be more difficult to track staff roles (especially staff with multiple roles) across several systems.

The important factor is to grant access based upon what staff need for their roles today, not what role they previously had or what role they may have do in the future. Staff should not have too many access rights or too few. They should have just the right amount to fulfil their role.

Too many rights could lead to an incident.

Too few rights, could prevent staff from fulfilling their roles

Managing access should be a continuous process.



About this graphic

This graphic shows the stages of the continuous process of managing access.

The stages of the cycle are generally:

- identify joiners, movers and leavers
- identify systems and roles, joiners, movers and leavers have/need access to
- identify whether to amend, create, suspend or delete user(s)
- implement desired account changes
- verify account changes

You should link these actions into your joiners, movers and leavers process so that changes can be made promptly. If you take a periodic approach, such as allocating access based on a monthly ESR report of joiners, movers and leavers, you should be aware of the risks associated with leaving this time window and the amount of time it takes to action the changes on your systems. For example, it may be acceptable to wait a month before disabling a viewing account on a non-sensitive system, such as for desk booking reporting, but it would not be acceptable to wait this long to disable an administrative account on a core system, such as a care record system.

Assurance

As well your regular processes for dealing with starters, movers and changers, there should be an intermittent user account audit (at least annual)

The audit should look at your user lists and roles for each system and reality, identifying changes or deleting / disabling.

You would expect such an audit to generate a work list as the simple example below:

User account audit				
Undertaken by	First name / Surname			
Audit location	Site B, IT Room	Date / Time	dd/mm/yy @ hh:mm	3rd Audit
	User account exception	Action	Allocated	Complete
1.	Finance System: Glen Ledger still has a live account despite leaving 2 weeks ago	Disable finance account passed to desktop to verify other systems	Finance System Manger, Desktop team	Y/N
2.	Windows Systems Dianne Dicom still has access to pathology drives despite moving to radiology 2 months ago	Desktop to remove access	Desktop Team	Y/N
3.	Windows Systems Pam Pathological who replaced Dianne Dicom in Pathology doesn't have access to pathology drives	Add access	Desktop Team	Y/N
4.	HR System Gill Grievance who should a normal user role has an administrative one probably due to mistaken account code with Gilmore Grievance HR Systems Manager	HR Systems Manager to reduced rights / investigate	HR Systems Manager	Y/N

Audit scope

The audit of systems should be scoped around those that contain personal sensitive information as defined in this document.

Incidents

Where a user has inappropriate or incorrect system access rights in relation to their role, this sometimes can lead to an incident. As mentioned, these can be when there are too many or too few rights. The organisation should have an open and honest culture, which encourages staff reporting of incidents and near misses so that the organisation can learn valuable lessons.

Examples of the type of incidents that could occur include:

- a clinician is unable to order blood tests due to insufficient rights
- a junior member of IT deletes various groups within Windows active directory accidentally due to too many rights, in this case domain administrator role
- a disgruntled ex-member of staff manages to log on remotely and make several offensive postings - this could happen due to leaving employee accounts not being revoked in a timely fashion
- a member of staff sends a sensitive report to what is thought to be a printer located nearby but it goes to a printer in the staff member's old department - this could be due to the account details of a member of staff not changing when they moved to a different department
- all members of staff can see a sensitive executive document - this could be due to staff having too many rights or the document too few

Logging

System logs are a vital part of security, allowing you to trouble shoot system performance and help alert and identify any anomalies that may indicate malicious activity. As such, logs are important records that need protecting.

In generating logging information, it should be recognised that the logs themselves are records in their own right. They can contain information that is just as sensitive (if not sometimes more sensitive) than the originating records.

They should have their own retention schedule and security considerations. This should be explained in a corporate policy on logging (though this can be encompassed in another policy).

The policy should consider:

- security of logs for authenticated users only
- ensuring that logs cannot be tampered with
- offline backup
- log files for servers and workstations
- internet access
- mobile devices and tablets
- out of area lookup (physical or IP address)
- out of hours lookup
- logins from multiple devices with one account

The policy should be organisational aware. That is, A&E will not have a concept of out-of-hours or remote users may login from various devices if using virtual desktops.

Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. Organisations should consider the ability to trace an incident end to end such as network address translation.

Guidance is available from the National Cyber Security Centre which will help you devise an approach to logging for security purposes.

It’s important to recognise that just retaining logs is of little value if they are not acted upon.

Account Removal

Many operating systems and information systems have categories and specific user accounts that by default provide access. These tend to have the same default identifier and password (if one exists at all).

A good example of this type of account is the guest account within Windows Active Directory or the guest session account in Ubuntu or Linux.

NCSC - Windows guidance

https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides/windows

NCSC - Ubuntu guidance

https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides/ubuntu-lts

As well as those system accounts, user accounts which are no longer needed (such as leavers) should be disabled or removed. This should be in conjunction with having a reviewed starters, movers and leaver process / policy as detailed in Big Picture Guide 5 Process Reviews.

Systems holding personal confidential information – Part 2 (4.3.1 – 4.5.5)

Systems administrators

Systems administrators by nature of their role have elevated rights compared to a normal user. Normal users' access can be restricted to role and limited to what they need to do to perform, therefore protecting the organisation and themselves.

Conversely, administrators do not have the same level of role limiting protection, so it falls to the individual. Systems administrators therefore have a great deal of system power and with great power comes great responsibility. The system administrator needs the highest level of integrity in terms of respect of the confidentiality, integrity or availability of the systems they support.

The CIA Triad

- **Confidentiality -** ensuring you only view what you need to administer the system and not disclose sensitive information.
- **Integrity -** ensuring you do not alter records inappropriately.
- **Availability -** ensuring that systems up time is kept as high as possible and all maintenance is agreed to local standards

Administrators should be accountable for that responsibility.

Systems administrators accounts (privileged access)

Use

Using an elevated account for high-risk activities such as reading email and browsing the web is a high-risk activity. This is because malware that can reside on emails or web pages can run with elevated access on that device.

For example, a single windows account used by an IT Administrator for general use Outlook and Chrome web browsing that is also a member of the Domain Admins group in Windows Active Directory. This account is also used to manage servers with Active Directory Users and Computers as well as other Active Directory applications.

Your organisation should only grant privileged access on devices owned and managed by your organisation. The devices in scope are end user endpoints (PCs and mobile devices) not servers.

If there are circumstances where this is not possible this should be explained or managed as part of your risk management process. Such as the systems' backend infrastructure being cloud based or managed as a service by 3rd parties on your behalf, however you may still have privileged access (at some level) to those devices/systems.

Logging

Privileged access users who have the highest level of access to systems can have a tremendous impact in resolving incidents when they occur, such as by reviewing changes made by a malicious attacker and reverting back to the original data. However, they can also unfortunately cause serious incidents due to their high level of access and increased responsibility.

In line with, and contained within, your logging policy, you should have the facility to store and retain all privileged user sessions for offline analysis and investigation. This will allow you as an organisation to examine the root cause analysis and identify areas for improvement.

Revocation

Due to the nature of these accounts having an elevated level of privileged access it is even more important that this level of access is revoked when no longer required.

This can be where the individual leaves the organisation or through role change (generally through disabling or deleting the administrative account). This is relatively simple to manage in line with any user (albeit it is more important it's done in a very timely fashion).

However, it is more difficult to monitor where an individual has not left or changed role but they no longer require escalated rights for that system. In such instances, users may accumulate rights resulting in administrator privilege creep.

Know your users, systems and devices

It's important that your organisation is clear about who (or what in the case of automated functions) has authorisation to interact with the network and information system.

For people this journey starts with employment checks prior to employment. However, digitally, our primary concern is identification and authentication prior to access.

Identification being a digital identifier that signifies who you are and authentication a method of proving so. The most common combination being a username and password.

For those critical systems under the Network and Information Systems (NIS) directive you should ensure multifactor or hardware authentication is enabled unless there is an exceptional (and documented) reason for it not to be.

It's important when identifying and authenticating 'things' (systems and devices), that things can have a higher threshold of identification and authentication than people.

For example, a device can have a longer identifier which is non guessable. It can also have a digital certificate. A system, such as a Windows account used in an automated script, can also have a longer identifier and an associated very high strength password.

Generally, authentication is expressed in 3 forms.

Type 1 – Something You Know – includes passwords, PINs, combinations, code words. Anything that you can remember and then type, say or do

Type 2 – Something You Have – includes all items that are objects, such as smart cards or tokens.

Type 3 – Something You Are – includes any part of you used for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

The more factors the stronger the authentication.

Read the NCSC guidance on identity and access management

Monitoring

Staff should understand that there is capability and capacity for their actions within systems to be monitored and recorded.

The more sensitive the system, the more granular and extensive the monitoring should be.

The type of activities that can be monitored include:

- creation of new items
- reading of items including navigating between items
- updating and modification of items
- deletion or disabling of items

- printing of items (what's printed and to where)
- exporting or saving items outside the system

Typical recording events would also include the date and time, the user account used, and the ID of the device used.

Examples of monitoring recording events include:

- recording when a new user is added to a theatre's system
- what patient records are viewed within a patient administration system
- a user account is disabled on a cardiology system
- a service users drug dosage is modified in a mental health administration system
- a clinical discharge letter is printed from a correspondence document management system

For each system, there should be an understanding of what events are monitored and how.

For example:

1. A theatre system monitors the creation, viewing modification, deletion of theatre slots, allocated patients and their demographics, movement of patients between slots and any administrative function, such as changing time units and turnaround between slots. This is through the proprietary system within the application developed by the supplier.
2. For Windows Active Directory, as well as the inbuilt Microsoft functionality, we employ a third-party tool XYZ that provides functionality logging against each administrator for their activity against all objects (CRUD), the schema and the ability to record and recover tomb stoned objects
3. We have many clinical systems by the same supplier (PAS, RIS, theatres, pathology and cardiology). They all have the same central Microsoft SQL monitoring system that can record all the common events (create, delete, update, view) for each record within the system. It can also look across systems to see who has interacted with a patient's records through any interaction with any of the systems. We produce and act upon management intelligence, such as most viewed patient across system (such as during a recent high-profile patient case), the most modified patient record, the most active users.

This information monitoring logging should be recorded against each system holding personal data. If you have an established and well-regarded information asset register, this information can be appended to that asset record.

The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel.

Staff awareness

Staff awareness that their actions are monitored within systems can have a positive effect on reducing the more dubious action some staff can take within systems.

It is important that staff are reminded of monitoring. Delivery can take many forms – it can be a discrete event or part of a wider employee induction. It can be delivered face to face or digitally. It can form part of an annual email reminder, a Windows login banner, a Windows background or screensaver or more traditionally with posters.

However you choose to make your staff aware of monitoring, it's important that it is effective and that you can measure that effectiveness.

Notification of staff can form part of your wider programme of staff guidance on confidentiality and data protection issues as covered in guide 1.

Passwords policy

You should have a password policy (either individual or part of a wider policy) that cover giving staff advice on managing their passwords.

As a minimum this should cover:

- how to avoid choosing obvious passwords (such as those based on easily-discoverable information)
- not to choose common passwords (use of technical means, using a password block is recommended
- no password reuse
- where and how they may record passwords to store and retrieve them securely e.g. through using a password manager
- if password management software is allowed, if so, which

NCSC guidance - Password administration for system owners

NCSC - enhancing usability case study

Technology

You should have technical controls in place that support and enforce your password policy and help prevent password guessing attacks.

The types of technical controls can be group policy in Windows Active Directory with a group policy on password length, password age and history.

You should also look at account lockout. For example, in Windows AD you can set the number of failed attempts (threshold) and length of time for the lockout duration. NCSC recommend between 5 and 10 login attempts before the account is frozen, to avoid accidental lockout.

Technical controls enforce password policy and mitigate against password-guessing attacks

Recently there has been a change in advice on not using complexity and not enforcing password expiry requirements on user passwords. This is to reduce burden on users, instead use a longer passphrase or avoid user generated password where possible (NCSC).

NCSC guidance - Password administration for system owners

Multifactor Authentication

Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.

The national MFA policy requires that organisations must enforce MFA on all remote access, and on all privileged accounts on external systems, and should enforce MFA on privileged accounts on internal systems. If you rely on any of the specific exceptions allowed by the policy, you must provide (within your response to this assertion) a summary of your internal approvals and your plans to minimise or eliminate those exceptions. Full detail is given in the policy and explanatory guidance.

System and Social Media Accounts

System accounts are those accounts not used by people but by systems. These can be standards in built-in system accounts, such as a Simple Network Management Protocol (SNMP) Community String or ones you create yourself such as an account in Windows AD, which requires domain admins rights to run several automated scripts.

These accounts should not use the default password such as public in the SNMP example.

You should remember that system accounts are not used by people so should not be bound by password attributes associated with people (they don’t have to be memorable). If the systems support it, they can be very long, very random and highly complex.

Systems or infrastructure with no concept of identity / accounts

There are devices (especially legacy ones) where there is no username and access is controlled through one password for that device. Generally, this password only login would give you extensive set rights as the device / system has no granularity of access, so it's all or nothing and it tends to be all.

For systems and devices falling into this category the password should be high strength.

Social Media Accounts

Given the accounts by their nature are very public, social media accounts can represent an easy way to hijack an organisation's public persona if weak or guessable passwords are used.

Social media should use passwords that are not easy to guess and are high strength.

You should avoid the top most leaked passwords.

3rd Party Account / Limited Access Management

You should have the ability to grant limited privileged access both in terms of scope and longevity.

This would be applicable to contractors and third parties undertaking a specific or time limited tasks.

This can take the form of an account with a shortened expiry date, an account which is used for the task then disabled (such as one during a remote support session) or using an account that uses a one-time password where you control the password generator.

Internet facing service and Internet facing authentication services

So those internet facing services including authentication services you use should utilise high strength passwords.

A high strength password, not guessable, not topmost leaked backed up with technical enforcement (such as using password blocklists). This should in line with current NCSC password guides.

NCSC - article about password deny lists

NCSC guidance - Password administration for system owners

Appendix 1 - Useful resources

Identity and access management:

NCSC - Control who and what can access your systems and data.

https://www.ncsc.gov.uk/collection/10-steps/identity-and-access-management

Advice and guidance:

NCSC - Expert, trusted, and independent guidance.

https://www.ncsc.gov.uk/section/advice-guidance/all-topics

Multi-factor authentication (MFA) policy:

This policy 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.

https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/multi-factor-authentication-mfa-policy

Appendix 2 – The National Data Guardian Reports

The NDG Report

Recommendations to improve security of health and care information and ensure people can make informed choices about how their data is used.

Review of Data Security, Consent and Opt-Outs

The government response

‘Your Data: Better Security, Better Choice, Better Care’ is the government’s response to:

- the National Data Guardian for Health and Care’s ‘Review of Data Security, Consent and Opt-Outs’
- the public consultation on that review
- the Care Quality Commission’s Review ‘Safe Data, Safe Care’.

It sets out that the government accepts the recommendations in both the National Data Guardian review and the Care Quality Commission review.

It also reflects on what we heard through consultation to set out immediate and longer-term action for implementation.

Your Data: Better Security, Better Choice, Better Care