NHS Digital

Data Security Standard 4

Managing data access

The bigger picture and how the standard fits in

2021/22

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 (e.g. sign in sheets, CCTV, correlation with other systems, shift rosters etc).

Systems holding personal confidential information

Definitions and scope from NDG report

Personal information is personal and in the context of health and care usually sensitive confidential information that is held (usually digitally) about staff and patients / service users. Confidential personal information is likely to include (but is not limited to) information about a person's:

- physical or mental health
- social or family circumstance
- financial standing and financial details
- education, training and employment experience
- religious beliefs
- racial or ethnic origin
- sexuality
- criminal convictions
- genomic data
- IP address.

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

- patient administration systems
- staff rostering systems
- payroll
- theatre systems
- data warehouses
- a clinical correspondence system.

Know your organisation

Know your staff

There should be a staff repository (normally within a HR department for larger organisations) of current staff and their roles. This repository should be up to date and reflect when staff are recruited, their change of role(s) or if they leave the organisation.

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.

Typically, in NHS organisations, the source of this information would be ESR (Electronic Staff Record).

An organisation can strengthen its approach by implementing and monitoring a strong joiners, movers and leavers policy (though this can be encompassed in another policy).

Your organisation maintains a record of staff and their roles.

Data Security Standard 4.1.1

Know your systems

This encompasses those systems that hold personal information (as defined) but also those that do not (holding more than 100 records).

Access to systems

There should be an understanding of who has access contained within the system. Access to the system might be managed by the system itself or use some form of federated access in which a single account is trusted across multiple IT systems – such as with Single Sign On (SSO).

Regardless of how this is managed, you should know who has access to the information within systems. If that information is shared with another system (such as through interfacing), you should know who has access to that system too. This standard is not interested in how access works (i.e. username and password, smartcard or biometric), just who has access to the information in systems.

Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?

Data Security Standard 4.1.2

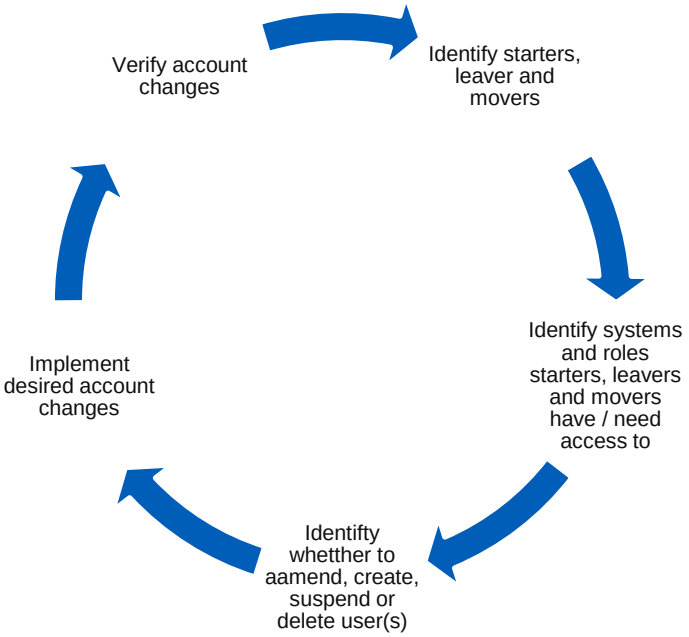
For each system using role-based access, an indication of what role exists within the system and the numbers of staff against each role. A simple example is given below:

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. So, in our example, 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, when the ‘view user’s’ role will allow them the 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 have access based upon what staff need for their roles today, not what role they previously had or what role they may do in the future. If you think of Goldilocks, staff should not have too many rights or too little, just right amount is best.

Managing access should be a continuous process.



If you take a periodic approach such as acting upon a monthly ESR starters, changes and leavers report with manual intervention on each system, you should be aware of the risks associated between the change and the time taken to action the change on each of your systems.

For example, not disabling a viewing account on a non-sensitive system may be acceptable within a month but an administrative account for a core system would typically not be.

Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?

Data Security Standard 4.1.3

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.

When was the last audit of user accounts held?

Data Security Standard 4.2.1

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.

Examples of the type of incidents that could occur are:

- a clinician is unable to order blood tests due to insufficient rights
- a junior member of IT deletes various groups within Windows active directory accidently 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.

Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.

Data Security Standard 4.2.2

Logging

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 greater) 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

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 e.g. network address translation.

Guidance is available from the National Cyber Security Centre which will help you devise an approach to logging for security purposeshttps://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes

https://www.ncsc.gov.uk/files/NCSC_SOC_Feeds.pdf (does not mandate a CSOC)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).

Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity.

Data Security Standard 4.2.3

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.

https://www.ncsc.gov.uk/collection/end-user-device-security/platform-specific-guidance/windows-10-1803-with-mobile-device-management

https://www.ncsc.gov.uk/collection/end-user-device-security/platform-specific-guidance/ubuntu-18-04-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.

Are unnecessary user accounts removed or disabled?

Data Security Standard 4.2.4

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.
- Availability ensuring that systems up time is kept as high as possible and all maintenance is agreed to local standards
- Integrity breach ensuring you do not alter records inappropriately.

Administrators should be accountable for that responsibility.

All system administrators have signed an agreement which holds them accountable to the highest standards of use.

Data Security Standard 4.3.1

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.

> The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular reading email and web browsing.
>
> Data Security Standard 4.4.2

Your organisation should only grant privileged access on devices owned and managed by your organisation. The devices in scope are end user endpoints (PC's 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

When incidents occur, privileged access users can have a tremendous impact on either resolving the issues and sometimes unfortunately in its inception.

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 of cause and 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 is 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 is 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 than 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 directive (NIS) you should consider multifactor or hardware authentication.

It is 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 e.g. 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.

https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management

Are users, systems and where appropriate, devices, always identified and authenticated prior to being provided access to information or systems?

Data Security Standard 4.3.2

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 monitoring can occur on:

- 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:

- 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.

The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation

Data Security Standard 4.4.3

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

For example:

- 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, e.g. changing time units, turnaround between slots etc. This is through the proprietary system within the application developed by the supplier
- 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
- 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 (e.g. during a recent high-profile patient case), the most modified patient record, the most active users, etc.

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. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.

Data Security Standard 4.4.1

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 the big picture 1 guide.

Have all staff been notified that their system use could be monitored?

Data Security Standard 4.3.3

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:-

(a) How to avoid choosing obvious passwords (such as those based on easily-discoverable information).

(b) Not to choose common passwords (use of technical means, using a password blocklist recommended).

(c) No password reuse.

(d) Where and how they may record passwords to store and retrieve them securely.

(e) If password management software is allowed, if so, which.

(f) Which passwords they really must memorise and not record anywhere.

https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

https://www.ncsc.gov.uk/case-study/enhancing-usability-chesterfield-borough-council

Do you have a password policy giving staff advice on managing their passwords?

Data Security Standard 4.5.1

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.

Insert 4.5.2 here? 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).

https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Multifactor Authentication

Wherever possible use multifactor authentication for end user and end point devices (i.e. not server console). (multifactor, as explained in Know your users, systems and devices earlier in this guide).

This can be a more traditional approach with a hardware token with a onetime password, biometric or a certificate on a device.

See

> Multifactor authentication is used [wherever technically feasible].
>
> Data Security Standard 4.5.3

https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

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 an SNMP Community String or ones you create yourself such as an account in Windows AD which requires domain admins rights in order 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 (i.e. they don't have to be memorable). If the systems supports it, these 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 topmost leaked passwords.

https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordTop100k.txt

> Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.
>
> Data Security Standard 4.5.4

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.

Does your organisation grant limited privileged access and third party access only for a limited time period, or is it planning to do so?

Data Security Standard 4.5.5

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 (i.e. using password blocklists). This should in line with current NCSC password guides.

https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere

https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Appendix 1 -
Table of Data Security Level 4 Assertions

Assertion	Sub Assertion	Evidence
4.1 The organisation maintains a current record of staff and their roles.	4.1.1	Your organisation maintains a record of staff and their roles.
	4.1.2	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?
	4.1.3	Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?
4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.	4.2.1	When was the last audit of user accounts held?
	4.2.2	Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.
	4.2.3	Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity.
	4.2.4	Are unnecessary user accounts removed or disabled?
4.3 All staff understand that their activities on IT systems will be monitored and recorded for security	4.3.1	All system administrators have signed an agreement which holds them accountable to the highest standards of use.
	4.3.2	Are users, systems and where appropriate, devices, always identified and authenticated prior to being provided access to information or system?
	4.3.3	Have all staff been notified that their system use could be monitored?
4.4 You closely manage privileged user access to networks and information systems	4.4.1	The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation

supporting the essential service.		information life cycle policy with disposal as appropriate.
	4.4.2	The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular email and web browsing.
	4.4.3	The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation.
4.5 You ensure your passwords are suitable for the information you are protecting	4.5.1	Do you have a password policy giving staff advice on managing their passwords?
	4.5.2	Technical controls enforce password policy and mitigate against password-guessing attacks.
	4.5.3	Multifactor authentication is used [wherever technically feasible].
	4.5.4	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.
	4.5.5	Does your organisation grant limited privileged access and third party access only for a limited time period, or is it planning to do so?

Appendix 2 - Useful resources

Access control in health and care organisations: NHS Digital Data Good Practice

Guidance on good practice in controlling access to NHS and health and care systems and services. The guidance covers physical access and access to:

https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/access-control

Guidance: National Cyber Security Centre

Expert, trusted, and independent guidance for UK industry, government departments, the critical national infrastructure and private SMEs. All our guidance is advisory in nature and is underpinned by our unique insights into cyber threats.

https://www.ncsc.gov.uk/guidance

Appendix 3 –
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