# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Systems holding personal confidential information</td>
<td>4</td>
</tr>
<tr>
<td>Definitions and scope</td>
<td>4</td>
</tr>
<tr>
<td>Know your organisation</td>
<td>5</td>
</tr>
<tr>
<td>Know your staff</td>
<td>5</td>
</tr>
<tr>
<td>Know your systems</td>
<td>5</td>
</tr>
<tr>
<td>Access to systems</td>
<td>5</td>
</tr>
<tr>
<td>Managing access should be a continuous process.</td>
<td>8</td>
</tr>
<tr>
<td>Assurance</td>
<td>9</td>
</tr>
<tr>
<td>Audit scope</td>
<td>9</td>
</tr>
<tr>
<td>Incidents</td>
<td>9</td>
</tr>
<tr>
<td>Systems administrators</td>
<td>10</td>
</tr>
<tr>
<td>Acceptable usage banner</td>
<td>11</td>
</tr>
<tr>
<td>Monitoring</td>
<td>13</td>
</tr>
<tr>
<td>Staff awareness</td>
<td>14</td>
</tr>
<tr>
<td>Appendix 1 -</td>
<td>15</td>
</tr>
<tr>
<td>Table of Data Security Level 4 Assertions</td>
<td>15</td>
</tr>
<tr>
<td>Appendix 2 -</td>
<td>16</td>
</tr>
<tr>
<td>Useful resources</td>
<td>16</td>
</tr>
<tr>
<td>Appendix 3 –</td>
<td>17</td>
</tr>
<tr>
<td>The National Data Guardian Reports</td>
<td>17</td>
</tr>
</tbody>
</table>
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.”

Users should not have access to data they have no business need to see – this is the principle of ‘least privilege’.

When it comes to IT systems, it is easy for staff to accumulate system accesses over time. To prevent this from happening, you should proactively manage user privileges (i.e. who has access to what). By doing this, there is a forensic trail back to a specific user or user group. This improves accountability. 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
Personal confidential information (PCI) is personal and usually sensitive confidential information that is held about staff and patients / service users. Personal confidential 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
- biometric data (i.e. fingerprints)
- IP address.

Confidential personal information would be held in systems such as:

- care planning systems
- staff rostering systems
- payroll.
Know your organisation

Know your staff

You should maintain a list of all staff and their roles. This should be up to date and reflect when staff are recruited, their change of role(s) or if they leave the organisation.

Know your systems

This encompasses those systems that hold personal confidential data (as defined) but also those that do not. This is also covered in Data Security Standard 2.

Access to systems

There should be an understanding of who has access to each system. Access to the system might be managed by the system itself – e.g. a rostering system where all staff can access a read-only view but only management can make alterations to rotas; or the multiple systems might be accessed by one person through a single account – e.g. a user logs on to the computer with their unique log-in and can access a rostering system, email and payroll.

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, e.g. if your rostering system provides information to a payroll system run by a third-party, you need to know who has access to that information as well.

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.

Each system should have role-based access. Role based access systems allocate user rights, dependent on what group or list you are a member of. For example, a user in an administrative group would be able to view, amend or delete everything, whereas someone in a read-only group could only view. For each system using role-based access, an indication of what role exists within the system and the numbers of staff against each role should be recorded. A simple example is given below:
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.

For small organisations which don’t use many systems, it might be easier to record each member of staff role against the staff list and what systems they have access to. For example:

<table>
<thead>
<tr>
<th>Name</th>
<th>Job title</th>
<th>Systems accessed</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patricia Personnel</td>
<td>Carer</td>
<td>Rostering system</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email</td>
<td>General</td>
</tr>
<tr>
<td>Colin Cloud</td>
<td>Data Security andProtection</td>
<td>Rostering system</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer network</td>
<td>Administrator</td>
</tr>
<tr>
<td>Susan Septum</td>
<td>Registered Manager</td>
<td>Rostering system</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Email</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Computer network</td>
<td>General</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Payroll</td>
<td>Administrator</td>
</tr>
</tbody>
</table>
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 have in the future. If you think of Goldilocks, staff should not have too many rights or too little, just right is best.

- **Too many rights** could lead to an incident
- **Too few rights**, staff cannot fulfil their roles
Managing access should be a continuous process

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

If you have a networked care planning system, ensure you delete or disable accounts after staff leave.
Assurance

As well your regular processes for dealing with starters, movers and changers, there should be an intermittent user account audit.

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

**MANDATORY:** Date last user accounts audit held.

Data Security Standard 4.2.1

Audit scope

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

Incidents

If a user role has a mismatch between itself and reality, sometimes this 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 carer is unable to access a service user’s care plan due to insufficient rights;
- a receptionist accidentally accesses details of other staff members pay details due to too many rights;
- a disgruntled ex-member of staff manages to log on remotely and make several offensive postings. This could happen due to employee accounts not being revoked in a timely fashion;
- 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.

**List of incidents caused by a mismatch between user role and system accesses granted.**

Data Security Standard 4.2.2
Systems administrators

A system administrator is typically responsible for installing, configuring and maintaining hardware and software infrastructure. It is likely that many small care providers will not have someone in this position in the organisation, or that the person fulfilling this role is a third-party contractor.

Systems administrators by nature of their role have elevated rights compared to a normal user. A normal user’s access can be restricted to their role and limited to what they need to do to perform their work. This protects the organisation and the member of staff.

Conversely, administrators do not have the same level of role limiting protection, because of the nature of their job. 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 the system up-time is kept as high as possible and all maintenance is agreed to local standards
- Integrity - ensuring you do not alter records inappropriately.

Administrators should be accountable for that responsibility. In recognition of this responsibility, your system administrators should sign a System Administrator Agreement. This should be incorporated with third-party contracts if you use external IT support.
Acceptable usage banner

It is important that staff know their responsibilities towards data security. They will need to have access to policies and guidance around this and, if they use IT, will need to sign an Acceptable Use Policy or similar.

Showing a banner before logging into a system can be an easy and effective way of reminding staff of their responsibilities prior to accessing a system. A banner is some text which pops up and has to be accepted prior to, or as part of, the login process. If it is not accepted then the system cannot be accessed.

The banner should remind staff of their personal accountability.

Some examples are:

- **Sample 1**

"Notice to All Users (Authorised or Unauthorised).

This computer system is for authorised use only. Users have no explicit or implicit expectation of privacy.

Any or all uses of this system and all data on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized sites and law enforcement personnel, as well as authorized officials of other agencies. By using this system, the user consent to such disclosure at the discretion of authorised site personnel. Unauthorized or improper use of this system may result in administrative disciplinary action, civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. STOP IMMEDIATELY!!! if you do not agree to the conditions stated in this warning.

+ Please refer the Company Policy document available in the 'Intranet'.
+ Contact HR (XXX) or IT Security Officer (XXX)"
Sample 2

"By clicking on the OK button below and logging into the (your company name here) domain, you agree to abide by the terms of the (your company name here) IT and Electronic Communications Policy. A copy of this policy can be viewed on the intranet.

The type of material you access on the Internet is strictly monitored and filtered. Users are responsible for ensuring that they act in accordance with this policy and other policies and legislation applicable to the (your company name here) network."

Sample 3

The following is an example banner provided by the Department of Justice:

"This system is for the use of authorised users only.

Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials."

Source: http://www.vulpoint.be/sample-log-on-warning-banner/

Acceptable IT usage banner displayed to all staff when logging into system, including a personal accountability reminder.

Data Security Standard 4.3.3
Monitoring

Staff should understand that their actions within systems are probably monitored and recorded. The more sensitive information the system contains, 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 system
- who has updated a care record in a care planning system
- a user account is disabled on a payroll system
- a service user's drug dosage is modified in a mental health administration system
- a rota is published on a rostering system.

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

- a rostering system monitors the creation, viewing, modification, deletion of shifts, allocated locations, holiday and sick leave. This is through the proprietary system within the application developed by the supplier;
- for desktop computers, each user has an individual log-in which allows them access to certain areas of the network based on their role. This is monitored by our IT support XYZ and the details outlined in our contract.

This information monitoring logging should be recorded against each system holding personal data. This information can be recorded in your information asset register.
**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 a discreet event or part of a wider employee induction. It can be delivered face to face or digitally. It can form part of 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 is effective and that you can measure that effectiveness.

**MANDATORY:** List of all systems to which users and administrators have an account, plus the means of monitoring access.

Data Security Standard 4.3.4

**MANDATORY:** Staff have provided explicit understanding that their activity of systems can be monitored.

Data Security Standard 4.3.5
### Appendix 1 -
**Table of Data Security Level 4 Assertions**

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Mandatory</th>
<th>Sub Assertion</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 The organisation maintains a current record of staff and their roles.</td>
<td>Yes</td>
<td>4.1.1</td>
<td>The organisation maintains a current record of staff and their roles.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>4.1.2</td>
<td>For each system holding personal and confidential data, the organisation understands who has access to the information.</td>
</tr>
<tr>
<td>4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.</td>
<td>Yes</td>
<td>4.2.1</td>
<td>Date last audit of user accounts held.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>4.2.2</td>
<td>List of incidents caused by a mismatch between user role and system accesses granted.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>4.2.3</td>
<td>Staff awareness - Access to information (Q13): The level of access I have to IT systems holding sensitive information, is appropriate.</td>
</tr>
<tr>
<td>4.3 All staff understand that their activities on IT systems will be monitored and recorded for security</td>
<td>Yes</td>
<td>4.3.1</td>
<td>All system administrators have signed an agreement which holds them accountable to the highest standards of use.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>4.3.2</td>
<td>The person with responsibility for IT confirms that IT administrator activities are logged and those logs are only accessible to appropriate personnel.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>4.3.3</td>
<td>Acceptable IT usage banner displayed to all staff when logging into system, including a personal accountability reminder.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>4.3.4</td>
<td>List of all systems to which users and administrators have an account, plus the means of monitoring access.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>4.3.5</td>
<td>Staff have provided explicit understanding that their activity of systems can be monitored.</td>
</tr>
</tbody>
</table>
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:


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

Care Provider Alliance

The Care Provider Alliance has provided template staff guidance and contract clauses.

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