Distinguished. World

Data Security Policy

Health and Social Care Act 2008 (Regulated Activities) Regulations 2014	**17, 19**

CQC Single Assessment Framework Topics

Safe Topic Areas:

Learning culture
Safeguarding
Safe environments
Safe and effective staffing

Effective Topic Areas:

Consent to care and treatment

Caring Topic Areas:

Kindness, compassion and dignity

Responsive Topic Areas:

Providing information

Well-led Topic Areas:

Shared direction and culture
Governance, management and sustainability

Please see the 'Quality Statements' section for full guidance

Scope

This 'Data Security Policy' regards the safeguarding and protection of sensitive personal information and confidential information as is required by law (including, but not limited to, the Data Protection Act 2018, Health & Social Care Act 2012 and 2015, and the Common Law duty of confidentiality).

This policy includes in its scope all data which we process, either in hardcopy or digital copy; this includes special categories of data. This policy applies to all staff, including temporary staff and contractors.

This policy and procedure are provided for the regulated activity of personal care.

Equality Statement

Our organisation is committed to equal rights and the promotion of choice, person-centred care and the promotion of independence. This policy demonstrates our commitment to creating a positive culture of respect for all individuals. The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability, sex, gender reassignment, pregnancy and maternity, race, sexual orientation, religion or belief, and marriage and civil partnership. It is also intended to reflect the Human Rights Act 1998 to promote positive practice and value the diversity of all individuals.

Key Points

- We have in place robust arrangements for the availability, integrity and confidentiality of data, records and data management systems. Information is used effectively to monitor and improve the quality of care.
- This policy includes in its scope all data which we process either in hardcopy or digital copy; this includes special categories of data.
- Physical access to records shall only be granted on a strict ‘Need to Know’ basis.

- Our staff must keep personal and confidential data securely in locked storage when not in use and keys should not be left in the barrels of filing cabinets and doors.
- All offices, when left unoccupied, must be locked unless all personal and confidential information has first been cleared from workstations/desks and secured in locked storage.
- Confidentiality audits will focus on controls within electronic records management systems and paper record systems, the purpose being to discover whether confidentiality has been breached or put at risk.
- In order to mitigate the risks of a security breach we will:
- Follow the Physical Access, Digital Access, Access Monitoring and Data Security procedures.
- Ensure our staff are trained to recognise a potential data breach whether it is a confidentiality, integrity or availability breach.
- The Data Security and Protection Lead and/or Registered Manager will inform any individual that their personal data has been breached if it is likely that there is a substantial risk to their rights and freedoms.

Policy Statement

The purpose of this document is to outline how we prevent data security breaches and how we react to them when prevention is not possible. By data breach we mean a security incident in which the confidentiality, integrity or availability of data is compromised. A breach can either be purposeful or accidental. This 'Data Security Policy' covers:

- Physical Access procedures
- Digital Access procedures
- Access Monitoring procedures
- Data Security Audit procedures
- Data Security Breach procedures

The Policy

The organisation is committed to the secure and safe management of all Personal Data and Sensitive Personal Data it holds about service users, family members and staff in its lawful pursuit of its business and the delivery of the regulated activity.

Physical Access Procedures

Physical access to records shall only be granted on a strict ‘Need to Know’ basis. During their induction each staff member who requires access to confidential information for their job role will be trained on the safe handling of all information and will be taught the procedures which govern how data is used, stored, shared and organised in our organisation. Growing and developing confident and skilled digital leaders will ensure the digital development of those they manage. Staff will be provided with annual update training on Information Governance, including data security.

Staff must retain personal and confidential data securely in locked storage when not in use and keys should not be left in the barrels of filing cabinets and doors. 0000

All offices, when left unoccupied, are locked unless all personal and confidential information has first been cleared from workstations/desks and secured in locked storage.

The Information Asset Register (IAR) contains the location of all confidential and sensitive personal information. Each storage location is risk assessed to ensure that the data is properly secured. This risk assessment forms part of the IAR.

A record is be kept of who has access to each storage location. This record can be found within the IAR.

An audit is completed at least annually by the Registered Manager, or delegated manager, to ensure that information is secured properly, and that access is restricted to those who have a legal requirement to use the information. The details of this audit are outlined in the Data Security Audit Procedures below.

Digital Access Procedures

Access shall be granted using the principle of ‘Least Privilege’. This means that every programme and every user of the system should operate using the least set of privileges necessary to complete their job. We will ensure that each user is identified by a unique user ID so that users can be linked to, and made responsible for, their actions.

The use of group IDs is only permitted where they are suitable for the work carried out.

During their induction each staff member who requires access to digital systems for their job role will be trained on the use of the system, given their user login details, and they will be required to sign to indicate that they understand the conditions of access. As discussed, Information Governance training updates will be provided annually.

A record is kept of all users given access to the system. This record can be found in the IAR in the Registered Manager’s Office.

In the instance that there are changes to user access requirements, these can only be authorised by the Data Security and Protection Lead or Registered Manager.

The IAR will contain the location of all confidential and sensitive personal information which is digitally stored.

We will follow robust password management procedures and ensure that all staff are trained in password management. Information Governance training updates will be provided annually.

As soon as an employee leaves, all their system logons are revoked. As part of the employee termination process, the Data Security and Protection Lead and/or Registered Manager is responsible for the removal of access rights from the computer system.

The Data Security and Protection Lead or Registered Manager will review all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted user accounts which are identified are disabled immediately and deleted unless positively reconfirmed.

When not in use all screens will be locked, and a clear screen policy will be followed.

Access Monitoring Procedures

The management of digital access rights is subject to regular compliance checks to ensure that these procedures are being followed and that staff are complying with their duty to use their access rights in an appropriate manner. Quarterly supervisions and spot checks will be used to assess compliance.

Areas considered in the compliance check include whether:

- Allocation of administrator rights is restricted
- Access rights are regularly reviewed
- There is any evidence of staff sharing their access rights; staff should know that this can result in disciplinary procedures
- Staff are appropriately logging out of the system
- Our password policy is being followed
- Staff understand how to report any security breaches

Data Security Audit Procedures (See 'Appendix')

Confidentiality audits will focus on controls within electronic records management systems and paper record systems. The purpose of these audits is to discover whether confidentiality has been breached, or put at risk, through deliberate misuse of systems, or as a result of insufficient controls.

Audits of security and access arrangements within each area are to be conducted on a six-monthly rolling programme. How frequently you audit information can vary, but as a minimum there should be a full annual audit.

Audits will be carried out as required by some or all of these methods:

- Unannounced spot checks to random work areas.
- A series of interviews with management and staff where a department or area of the organisation have been identified for a confidentiality audit.
- These audits will be carried out by the Data Security and Protection Lead or Registered Manager.

Information will usually be based on electronic reports from the care planning software, auditing of care plans and other relevant documentation, e.g. MAR records, either from our ICT contractor or from internal monitoring.

Some or all of the following checks will be made during data security audits:

- The Information Asset Register has been reviewed, updated and signed off.
- The Record of Processing Activities has been reviewed, updated and signed off.
- Failed attempts to access confidential information.
- Repeated attempts to access confidential information.
- Access of confidential information by unauthorised persons.
- Previous confidentiality incidents and actions, including any disciplinary action taken.
- Staff awareness of policies and guidelines concerning confidentiality and understanding of their responsibilities regarding confidentiality.
- Appropriate communications with service users.
- Appropriate recording and/or use of consent forms.
- Appropriate allocation of access rights to confidential information, both hardcopy and digital.
- Appropriate staff access to physical areas.
- Storage of, and access to, filed hardcopy service user notes and information.
- Correct process used to securely transfer personal information by post, fax or email.
- Appropriate use and security of desk and mobile devices in open areas.
- Security applied to PCs, laptops and mobile electronic devices.
- Evidence of secure waste disposal.
- Appropriate transfer and sharing arrangements are in place.
- Security and arrangements for recording access applied to manual files both live and archive, e.g. storage in locked cabinets/locked rooms.
- Appropriate staff use of computer systems, e.g. no excessive personal use, no attempting to download software without authorisation, use of social media, attempted connection of unauthorised devices etc.

Each audit will include a list of the activities undertaken, and action plans will be developed from the results to develop and improve data security and management.

Data Security Breach Procedures

In order to mitigate the risks of a security breach the organisation will:

- Follow the Physical Access, Digital Access, Access Monitoring and Data Security procedures.
- Ensure our staff are trained to recognise a potential data breach whether it is a confidentiality, integrity, or availability breach.
- Ensure our staff understand the procedures to follow and how to escalate a security incident to the correct person in order to determine if a breach has taken place.
- In the instance that it appears that a data security breach has taken place, the staff member who notices the breach, or potential breach, will complete a Data Security Incident Form without delay.
- This form will be completed and handed to the Data Security and Protection Lead or Registered Manager or, if they are not available, to a member of senior management.
- The Data Security and Protection Lead and/or Registered Manager will complete the rest of the Data Security Incident Form and conduct a thorough investigation into the breach.

Personal Data Breach

In the instance that the breach is a personal data breach and it is likely that there will be a risk to the rights and freedoms of an individual then the Information Commissioner's Office (ICO) will be informed as soon as possible, but at least within 72 hours of our discovery of the breach, via the 'DSPT Incident Reporting Tool.'

Also see 'NHS - Data Security and Protection Toolkit.'

As part of our report, we will provide the ICO with the following details:

- The nature of the personal data breach (i.e. confidentiality, integrity, availability).
- The approximate number of individuals concerned and the category of individual (e.g. employees, mailing lists, service users).
- The categories and approximate number of personal data records concerned.
- The name and details of our Data Security and Protection Lead or Registered Manager.
- The likely consequences of the breach.
- A description of the measures taken, or which we will take, to mitigate any possible adverse effects.

The Data Security and Protection Lead and/or Registered Manager will inform any individual that their personal data has been breached if it is likely that there is a high risk to their rights and freedoms. We will inform them directly and without any undue delay.

A data security breach must be marked on the IAR and will prompt an audit of all processes in order to correct any procedure which led to the breach.

A record of all personal data breaches will be kept including those breaches which the ICO were not required to be notified about.

Responsibilities

The Data Security and Protection Lead or the Registered Manager is responsible for physical security, updating and auditing the IAR and Records of Processing Activities (ROPA), digital access, managing breaches and data security audits.

*Please note this policy has been updated from the '**Digital Care Hub Data Security template**.'*

Cyber Essentials Technical Control Themes

If the organisation is bidding for public sector contracts which involve handling sensitive and personal information or the provision of certain technical products and services, they will require Cyber Essentials Certification.

The following link sets out guidance from the National Cyber Security Centre on IT infrastructure, 'Cyber Essentials: Requirements for IT infrastructure v3.1.'

The Data Security and Protection Lead or the Registered Manager will ensure that the following technical controls are in place in compliance with the Cyber Essentials requirements. This is particularly important where Cyber Essentials is a requirement of a publicly awarded contract from local government or NHS.

Please see 'Updates to the Cyber Essentials Scheme.'

Firewalls

Firewalls will be in place within the organisation to protect from unwanted access to the company's IT systems and networks. The firewalls will monitor all network traffic to identify and block unwanted traffic that could be harmful to the IT systems and networks. The security provided by the firewall will be adjusted to protect boundary firewalls, desktop computers, laptops, routers, servers, and cloud services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

The aim is to make sure that only secure and necessary network services can be accessed from the internet.

As all devices run network services to allow them to communicate with other devices and services, we aim to restrict access to these services, to reduce exposure to attacks from external software and hackers.

This is done by using firewalls or network devices with firewall functionality. For cloud services employed by the organisation we will consider/implement data flow policies to restrict access.

A boundary firewall is a network device which restricts the inbound and outbound network traffic to services on its network of computers and mobile devices. These will be used to protect against cyber attacks by implementing restrictions i.e. 'firewall rules,' which will allow or block traffic depending on its source, destination and type of communication protocol.

Where the organisation does not control the network to which a device connects, we will deploy and configure a software firewall to protect the device.

The organisation will:

- Protect every appropriate device with a correctly configured firewall (or network device with firewall functionality).
- Where installed, we will deploy the desktop or laptop operating system's software firewall in preference to a third-party firewall application.

For all firewalls (or network devices with firewall functionality), we will:

- Change default administrative passwords to a strong and unique password (see 'Password-based Authentication') – or disable remote administrative access entirely.
- Prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls:
- Multi-factor authentication (see MFA details below).
- An IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication system.
- Block unauthenticated inbound connections by default.
- Ensure inbound firewall rules are approved and documented by an authorised person and include the business need in the documentation.
- Remove or disable unnecessary firewall rules quickly, when they are no longer needed.
- Make sure we use a software firewall on devices which are used on untrusted networks, such as public wifi hotspots.

Secure Configuration

Secure configuration will be applied to servers, desktop computers, laptops, tablets, mobile phones, thin clients, IaaS, PaaS and SaaS.

This will be done to ensure that computers and network devices are properly configured to:

- Reduce vulnerabilities
- Provide only the services required to fulfil their role

The default configurations of computers and network devices are not always secure because out-of-the-box configurations often include one or more weak points such as:

- An administrative account with a pre-set, publicly known default password or without multifactor authentication enabled.
- Pre-enabled but unnecessary user accounts (sometimes with special access privileges).
- Pre-installed but unnecessary applications or services.

These default installations can allow attackers to gain unauthorised access to the organisation's sensitive information. Therefore, the organisation will apply technical controls when installing computers and network devices, to minimise vulnerabilities and protect against common types of attack.

The organisation will manage all computers and network devices by:

- Removing and disabling unnecessary user accounts (such as guest accounts and administrative accounts that will not be used).
- Changing any default or guessable account passwords (see 'Password-based Authentication').
- Removing or disabling unnecessary software (including applications, system utilities and network services).
- Disabling any auto-run feature which allows file execution without user authorisation (e.g. when they are downloaded).
- Ensuring users are authenticated before allowing them access to organisational data or services.
- Ensuring appropriate device locking controls (see 'device unlocking' below) for users that are physically present.

Device Unlocking Credentials

If a device requires a user's physical presence to access a device's services (such as logging on to a laptop or unlocking a mobile phone), a credential such as a biometric, password or PIN will be in place before a user can gain access to the services.

The organisation will protect the chosen authentication method chosen (e.g. biometric authentication, password or PIN) against brute-force attacks.

Where it is possible to configure within the software, the organisation will apply one of the following depending on the functionality:

- ‘Throttling' the rate of attempts, so that the number of times the user must wait between attempts increases with each unsuccessful attempt. You should not allow more than 10 guesses in five minutes.
- Locking devices after more than 10 unsuccessful attempts.

When the software is provided by a third party, and the vendor does not allow configuration of the above, we will use the vendor’s default setting.

Technical controls will be used to manage the quality of credentials. Where credentials are used to unlock a device, we will use a minimum password or PIN length of at least six characters.

When the device unlocking credentials are also used for authentication, we will apply the full password requirements to the credentials described in the section below for ‘user access controls.’

Security Update Management

Security update management is applicable to servers, desktop computers, laptops, tablets, mobile phones, firewalls, routers, IaaS, PaaS and SaaS.

The organisation aims to ensure that devices and software are not vulnerable to known security issues for which fixes are available.

Any device that runs software can contain security flaws, known as vulnerabilities. Vulnerabilities are regularly discovered in all types of software.

Once discovered, malicious individuals or groups often move quickly to misuse (or ‘exploit’) vulnerabilities to attack computers and networks.

It is important to note that software vendors provide fixes for vulnerabilities identified in products that they still support, in the form of software updates known as ‘patches’ or security updates. These may be made available to customers immediately or on a regular release schedule, e.g. monthly.

As an organisation we will make sure that all software is kept up to date and will:

- Be licensed and supported.
- Removed from devices when it becomes unsupported or removed from scope by using a defined subset that prevents all traffic to/from the internet.
- Have automatic updates enabled where possible.

- Be updated, including applying any manual configuration changes required to make the update effective, within 14 days of an update being released, where:
- The update fixes vulnerabilities described by the vendor as ‘critical’ or ‘high risk.’
- The update addresses vulnerabilities with a Common Vulnerability Scoring System (CVSS) v3 base score of 7 or above.
- There are no details of the level of vulnerabilities the update fixes provided by the vendor.

For optimum security it is advised by Cyber Essentials that all released updates are applied within 14 days of release (this is not mandatory). It is important that updates are applied as soon as possible, and 14 days is considered a reasonable period. Any longer would constitute a serious security risk while a shorter period may not be practical. Some vendors release security updates for multiple issues with differing severity levels as a single update. If such an update covers any ‘critical’ or ‘high risk’ issues then it should be installed within 14 days.

Sometimes the vendor will use different terms to describe the severity of vulnerabilities, see the precise definition in the Common Vulnerability Scoring System (CVSS).

For the purposes of the Cyber Essentials scheme, ‘critical’ or ‘high risk’ vulnerabilities are those with a CVSS3 score of 7 or above or are identified by the vendor as ‘critical or high risk.’

User Access Control

User access controls are applicable to all servers, desktop computers, laptops, tablets, mobile phones, IaaS, PaaS and SaaS.

The organisation uses user access controls to ensure that user accounts:

- Are assigned to authorised individuals only.
- Provide access to only those applications, computers and networks the user needs to carry out their role.

Every active user account in the organisation facilitates access to devices and applications, and to sensitive business, and potentially personal, information. Only authorised individuals will be assigned access to user accounts and will only be granted as much access as they need to carry out their role. This supports the organisation in reducing the risk of information being stolen or damaged or breaches of confidential information.

Compared to normal user accounts, accounts with special access privileges have enhanced access to devices, applications and information, e.g. IT administrators. If these accounts are compromised, an attacker could take advantage of the greater accesses to corrupt information on a large scale, disrupt business processes, access personal data or gain unauthorised access to other devices in the organisation.

Administrative accounts are especially highly privileged, for example. These accounts typically allow the user to:

- Execute software that can make significant and security-related changes to the operating system.
- Make changes to the operating system for some or all users.
- Create new accounts and allocate privileges.

All administrators will have this kind of account, including domain administrators and local administrators. This is important because if a user opens a malicious URL or email attachment, the malware would typically be executed with the same privilege level of the user's account.

This is why the organisation will take special care allocating and using privileged accounts.

The organisation will control all user accounts, especially those with access privileges that allow access to your organisational data and services. This also includes third party accounts, e.g. accounts used by support services.

The organisation will:

- Have in place a process to create and approve user accounts.
- Authenticate users with unique credentials before granting access to applications or devices (see 'Password-based Authentication').
- Remove or disable user accounts when they are no longer required (e.g. when a user leaves the organisation or after a defined period of account inactivity).
- Implement MFA, where available.
- Authentication to cloud services will always use MFA.
- Use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks).
- Remove or disable special access privileges when no longer required (e.g. when a member of staff changes role).

Password-based Authentication

All user accounts require the user to authenticate and where this is carried out using a password, the organisation will put in place the following protective measures:

- Passwords are protected against brute-force password guessing by implementing at least one of the following:
- Multi-factor authentication (see below).
- 'Throttling' the rate of attempts, so that the number of times the user must wait between attempts increases with each unsuccessful attempt. The organisation will not allow more than 10 guesses in five minutes.
- Locking devices after no more than 10 unsuccessful attempts.

- Use technical controls to manage the quality of passwords. This will include one of the following:
- Using multi-factor authentication (see below).
- A minimum password length of at least 12 characters, with no maximum length restrictions.
- A minimum password length of at least eight characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.
- We will aim to support users to choose unique passwords for their work accounts by:
- Educating people about avoiding common passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers.
- Encouraging people to choose longer passwords by promoting the use of multiple words (a minimum of three) to create a password (such as the NCSC’s guidance on using three random words).
- Providing usable secure storage for passwords (e.g. a password manager or secure locked cabinet) with clear information about how and when it can be used.
- Not enforcing password complexity requirements.

The Data Security and Protection Lead or the Registered Manager will ensure that passwords will be promptly changed where it is known or suspected a password or account has been compromised.

Multi-factor Authentication (MFA)

As well as providing an extra layer of security for passwords that are not protected by the other technical controls, the organisation will use multi-factor authentication to give administrative accounts and accounts that are accessible from the internet extra security.

The password element of the multi-factor authentication approach will have a password length of at least eight characters, with no maximum length restrictions.

There are four types of additional factor which will be considered:

- A managed/enterprise device
- An app on a trusted device
- A physically separate token
- A known or trusted account

Additional factors may be chosen so that they are usable and accessible.

For more information see ‘NCSC’s guidance on MFA.’

Malware Protection

Malware protection applies to all servers, desktop computers, laptops, tablets, mobile phones, IaaS, PaaS and SaaS.

The organisation's aim is to restrict execution of known malware and untrusted software, from causing damage or accessing data within the company's IT systems and networks.

Malware, such as computer viruses, worms and ransomware, is software that has been written and distributed deliberately to perform malicious actions. Potential sources include malicious email attachments, downloads (including those from application stores), and direct installation of unauthorised software.

Infected systems within the organisation are likely to suffer from problems like malfunctioning systems, data loss, or onward infection that goes unseen until it causes harm elsewhere or across the whole network.

The organisation will aim to avoid the potential for harm by:

- Preventing malware from being delivered to devices
- Preventing malware from running on devices

The organisation will ensure that a malware protection mechanism is active on all devices.

For each device, the organisation will use at least one of the options listed below, either using built in features in the software supplied or by purchasing products from a third-party provider.

In all cases the anti-malware software will be active, kept up to date in accordance with the vendor's instructions, and configured to work as detailed below:
Where we use anti-malware software to protect devices it will be configured to:

- Be updated in line with vendor recommendations
- Prevent malware from running
- Prevent the execution of malicious code
- Prevent connections to malicious websites over the internet

The devices will be configured to only allow approved applications, which are restricted by code signing, execute on devices.

We will:

- Actively approve such applications before deploying them to devices.
- Maintain a current list of approved applications, users must not be able to install any application that is unsigned or has an invalid signature.

Backing Up Data

Backing up means creating a copy of your information and saving it to another device or to cloud storage (online).

Backing up regularly means the organisation will always have a recent version of important and business critical information saved. This will help the organisation to recover quicker if your data is lost or stolen. Where available the organisation will turn on automatic backup to regularly save information into cloud storage, without you having to remember.

Where we back up information to a USB stick or an external hard drive, it will be disconnected it from computers or networks when a backup is not being done.

Backing up data is not a technical requirement of Cyber Essentials, however it is highly recommended as part of business continuity planning.

References and Further Reading

Data Security and Protection Toolkit, NHS Digital

Digital and data-driven health and care technology, A guide to good practice for the use of digital technology in health and care

Data security: local support, national webinar and film series, Digital Care Hub

NCSC's guidance on MFA

NCSC's guidance on using three random words

Common Vulnerability Scoring System (CVSS)

Updates to the Cyber Essentials Scheme

Cyber Essentials: Requirements for IT infrastructure v3.1

Quality Statements

Learning culture

We have a proactive and positive culture of safety based on openness and honesty, in which concerns about safety are listened to, safety events are investigated and reported thoroughly, and lessons are learned to continually identify and embed good practices.

Safeguarding

We work with people to understand what being safe means to them as well as with our partners on the best way to achieve this. We concentrate on improving people's lives while protecting their right to live in safety, free from bullying, harassment, abuse, discrimination, avoidable harm and neglect. We make sure we share concerns quickly and appropriately.

Safe environments

We detect and control potential risks in the care environment. We make sure that the equipment, facilities and technology support the delivery of safe care.

Safe and effective staffing

We make sure there are enough qualified, skilled and experienced people, who receive effective support, supervision and development. They work together effectively to provide safe care that meets people's individual needs.

Consent to care and treatment

We tell people about their rights around consent and respect these when we deliver person-centred care and treatment.

Kindness, compassion and dignity

We always treat people with kindness, empathy and compassion and we respect their privacy and dignity. We treat colleagues from other organisations with kindness and respect.

Providing information

We provide appropriate, accurate and up-to-date information in formats that we tailor to individual needs.

Shared direction and culture

We have a shared vision, strategy and culture. This is based on transparency, equity, equality and human rights, diversity and inclusion, engagement, and understanding challenges and the needs of people and our communities in order to meet these.

Governance, management and sustainability

We have clear responsibilities, roles, systems of accountability and good governance. We use these to manage and deliver good quality, sustainable care, treatment and support. We act on the best information about risk, performance and outcomes, and we share this securely with others when appropriate.

Key questions and quality statements - Care Quality Commission

Appendix: Data Security Audit Checklist

Staff	**Date audited**
Spot check that staff understand their responsibility towards data security	
Spot check that staff are aware of our data protection policies	
Have staff received training on data protection?	
Have any staff undergone disciplinary action in relation to data protection and security?	
Spot check that staff understand how to report security breaches and near misses.	
Physical Access to Hardcopy Records	
Check the record of which staff have access to confidential areas is up to date.	
All offices, files, or cabinets which contain confidential information are kept locked when not in use.	
Has all confidential waste been disposed of securely and are there destruction certificates? (If applicable)	
Has anyone inappropriately accessed, or attempted to access, confidential records?	
Digital Access to Records	
Is the allocation of administrator rights restricted?	
Have staff access rights been reviewed?	
Check if there is any evidence of staff sharing access rights.	
Screens are locked when not in use.	
Check that our password policy is being followed	
Has anyone inappropriately accessed, or attempted to access, confidential records?	
Have appropriate security measures been applied to all computers, laptops and mobile devices?	
Staff are using computers appropriately, e.g. no personal use, no downloading unapproved software, no social media use etc.	
Sharing Data	
Our procedures for safely sharing personal information via post are being followed.	
Our procedures for safely sharing personal information via fax are being followed.	

Our procedures for safely sharing personal information via secure email are being followed.	
Legal Checks	
The Information Asset Register has been reviewed and signed off.	
The Record of Processing Activities has been reviewed and signed off.	
Records of consent are up to date and still applicable.	