Distinguished. World

Confidentiality Policy (England Community)

Health and Social Care Act 2008 (Regulated Activities) Regulations 2014	**9, 10, 11, 16, 17**

CQC Single Assessment Framework Topics

Safe Topic Areas:

Safeguarding

Caring Topic Areas:

Kindness, compassion and dignity

Responsive Topic Areas:

Providing information

Well-led Topic Areas:

Governance, management and sustainability

Please see the 'Quality Statements' section for full guidance

Scope

This policy includes all staff and contractors who are bound by a legal duty of confidence to protect personal information (including Special Category Data as defined in General Data Protection Regulations (GDPR)) they may come into contact with during the course of their work. This means that staff are obliged to keep any Personal Identifiable Data (sometimes referred to as PID), strictly confidential, e.g. medical and employee records.

It should be noted that staff also come into contact with non-person identifiable information which should also be treated with the same degree of care. Some data may be confidential to the organisation, and this again must be treated in confidence, e.g. new marketing campaigns, financial information.

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 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

- All staff/contractors are responsible for maintaining the confidentiality of information gained during their employment/involvement with the organisation and this extends after they have left the employ of the organisation.
- Much of this information is highly personal and sensitive. We recognise that our service users have a right to privacy and dignity, and that this extends to our handling information about them in ways which cause as little as possible intrusion on those rights.
- We will only break the rule of confidentiality in very extreme circumstances which justify our taking that action for the greater good of a person using the service or, exceptionally, others in accordance with the Data Protection Act 2018 Code of Practice.
- The Data Protection Act lays various obligations on this organisation and similar organisations concerning the handling of the information we hold on individuals.
- Staff must receive information, training and support to understand their role in maintaining confidentiality and data protection.
- Records must be prepared, maintained and used in accordance with data protection legislation.
- A clear desk policy is keeping personal information secure and restricted to the minimum number of viewers possible. When you leave your desk, you should ensure that any personal or confidential information is not left lying around, or accessible via an unlocked computer screen for others to see.

Policy Statement

As an organisation we comply with The Data Protection Act 2018 (DPA) and GDPR concerning confidentiality within the organisation and the services it delivers. It is essential that all information we hold, about any of our service users using the service and staff, is not disclosed without their permission. This includes withholding information from families if the service user requests it.

In addition, the organisation is aware of its responsibility to share information fairly and proportionately in line with the Data Protection Act section 121. The organisation will share information where there is a need to protect, safeguard and support the health and well-being of the service user or carer, and where it would be more harmful not to share information.

Confidentiality of Information

All staff/contractors are responsible for maintaining the confidentiality of information gained during their employment and or involvement with the organisation and this extends after they have left the employ of the organisation.

Definition of Confidential Information

Confidential information can be anything that relates to service users, team members, their family or friends, or the business of the organisation, however stored. For example, information may be held on paper, USB pen, CD, computer file or printout, video, photograph or even heard by word of mouth. It includes information stored on portable devices such as laptops, palmtops, USB pens, mobile phones and digital cameras. It also includes any organisation confidential information such as the service business information.

The Policy

It is the aim of the organisation to manage all confidential information about individuals who may meet the organisation during the delivery of its services in compliance with all relevant legislation and regulations.

The work of the organisation inevitably involves the need-to-know personal details about our service users and their families or carers. The information is required to provide safe, effective, caring, responsive and well-led care and support to the service users.

Much of this information is highly personal and sensitive. We recognise that our service users using the service have a right to privacy and dignity, and that this extends to our handling information with

minimal intrusion and impact on the service user or their families.

Service Delivery

We want our service users to feel at ease with the staff that care for them. An important element in that relationship is the sharing of information with staff, confident that it will be used with appropriate respect and only in relation to the care provided.

Information within the organisation about individual service users will only be shared and provided to those staff who need the information to be able to care and support them, provide management and administration functions in the delivery of the service and other relevant tasks to ensure their needs are being met.

The organisation will share information where there is a need to protect, safeguard and support the health and well-being of the service user or carer, and where it would be more harmful not to share information. Staff and the organisation will always work in the best interests of the service user and will share information in line with the DPA 2018 Code of Practice. Where a service user lacks capacity to consent to sharing information, staff will work in accordance with the Mental Capacity Act 2005 to ensure that any information shared is done so in the person's best interests.

As part of the contract with the service user (self-funding service users), and a separate confidentiality agreement for local authority/health referrals, the organisation will agree where and how information can be shared and under which circumstances. Examples of people information may be shared with include:

- Their GP or other health care professionals treating the service user
- Their Care Manager/Social Worker
- Social care colleagues who are also working with this person using the service
- Other care providers jointly providing services
- Office staff and managers
- CQC inspectors
- Local authority/health commissioners

Examples of people you may not share information or discuss the service user with include your family and friends and your colleagues not involved in the service users' care.

Our Legal Obligations

Data Protection Act 2018

The DPA 2018 lays various obligations on this organisation and similar organisations concerning the handling of the information we hold on individuals. Information must, for example, be obtained fairly and lawfully, be held for specified purposes, be adequate, relevant and not excessive for the purpose for which it was gathered, be accurate and up to date, and not be held for longer than is necessary. We observe all of these requirements.

CQC

CQC has in place the Fundamental Standards which are minimum standards of care for the delivery of services within a regulated activity. These require organisations manage personal information sensitively, confidentially, and appropriately, including respecting the privacy of service users.

CQC requires organisations to have in place policies and procedures for the sharing of information between staff and other agencies (see the 'Working with Other Care Providers Policy'), managing confidential information, breaches of confidentiality, and the storage and administrative handling of confidential material and records.

Please also see:

- Data Protection and GDPR Policy
- Data Quality Policy
- Data Security Policy
- Record Keeping Policy

Information and Care Needs Assessment

Every person using the service must have their care needs thoroughly assessed before services are provided, with a care plan developed and in place to ensure their needs are identified and met.

Staff who carry out an assessment, or handle assessment/care planning or other material sent to us from other agencies, have access to personal and confidential information about a service user.

It is the duty of such staff to retain, record and share through the care plan and other documents, the information care workers require to meet the service users care and support needs. A similar obligation applies to staff involved in a review or reassessment of care needs or in making any changes in the service provided or escalating concerns to health or social care professionals.

The person using the service has the right to see their records and should be asked to check they agree with everything written in their personal care and support plan before being asked to agree and sign it.

Handling of Information by Care Workers

The care workers assisting a service user has access both to the information passed to them when they start to work with that service user and knowledge which accumulates in the course of providing care. They have a duty of confidentiality:

- To treat all personal information with respect and in the best interests of the service user to whom it relates.
- To share with their manager, when appropriate, information given to them in confidence if there are concerns or changing needs of the service user.
- To share pertinent confidential information when required with colleagues with whom they are sharing the task of providing care.
- To pass and receive confidential information to and from colleagues on occasions when they have to be replaced because of sickness, holidays or other reasons, in a responsible and respectful manner.
- Only to pass confidential information to other social and healthcare professionals/agencies with the agreement of the service user, with the permission of their manager, or in emergencies when it is clear that it is in the interests of the person using the service or is urgently required for the protection of the person using the service or another person (i.e. compliant with DPA 2018 Code of Practice).
- To refer to confidential information in training or group supervision sessions with respect and caution and in ways which conceal the identity of the service user to which it relates.
- Never to gossip about a service user or to pass information to any other individual other than for professional reasons.
- It is a condition of employment that staff do not disclose confidential information to an unauthorised person. Depending on the breach this could be classed as gross misconduct and lead to a disciplinary matter, and even dismissal (see the 'Disciplinary Policy').

Managerial and Administrative Responsibilities

Confidential information must occasionally be seen by staff other than the care workers providing direct care. It is therefore the responsibility of managers to ensure that information is stored and handled in ways that limit access to those who have a need to know, and to provide the following arrangements in particular:

- To provide lockable filing cabinets to hold service users' records and ensure that records are kept secure at all times.
- To arrange for information held on computers to be accessed only by appropriate personnel, e.g. through the use of password protection which allows only access to pertinent files relevant to the individual's role.

- To locate office machinery and provide appropriate monitor shielding so that screens displaying personal data are hidden from general view.
- To ensure paperwork is not left lying where anyone can read it.
- To ensure paperwork is not taken from the office unless absolutely necessary.

Exceptional Breaches of Confidentiality

There are rare occasions on which it is necessary for a staff member, acting in good faith to breach confidentiality in an emergency situation, for example to protect the service user or another person from grave danger without obtaining the permission of the person to whom it applies.

In such a situation, the staff member should use their best judgment, should consult the service user's representative, a manager or a colleague if possible, and should inform their manager of what has happened as soon as possible.

As discussed, the organisation will share information where there is a need to protect, safeguard, and support the health and well-being of the service user or carer, and where it would be more harmful not to share information. Staff and the organisation will work in the best interests of the service user and will share information in line with the DPA 2018 Code of Practice.

Right of Access

All people have a right to ask an organisation what information that organisation holds on them, and this is called a Subject Access Request (SAR).

The organisation must comply with a SAR without delay and at the latest within one month of receipt of the request or within one month of the receipt of any information requested to confirm the requester's identity.

All staff should be aware of the following with regards to requests for information from third parties:

- Never give out information about service users or team members to others, but pass the SAR request to the Registered Manager.
- All requests for person identifiable data other than from those engaged in the care of the individual are classed as Subject Access Requests. As a result, the Registered Manager or other appropriate data controller should be notified as soon as possible, as such requests must be complied with within strict statutory timescales.

Telephone Enquiries

If a request for information is made by telephone, all team members should:

- Always try to check the identity of the caller.
- Check whether they are entitled to the information they request.
- Take a number, verify it independently and call back if necessary.
- This includes requests by people claiming to be officials, e.g. Police or CQC inspectors.

Requests for Information by the Police and Media

Requests for information from the Police or media should always be referred to the Manager in the first instance, and Caldicott Guardian, senior manager or director where appropriate.

WARNING

If the Crime and Disorder Act 1998 is being implemented the full contact details of the police officer in charge of the case should be obtained and the request be passed to the Registered Manager who will escalate to appropriate members of the senior management team.

Clear Desk Policy

In order to comply with the Data Protection Act, a clear desk policy must be enforced. A clear desk policy is keeping personal information secure and restricted to the minimum number of viewers possible. When you leave your desk, you should ensure that any personal or confidential information is not left lying around for others to see. Lock it away in a cupboard or drawer if leaving your desk. Computers should be switched to screen lock as a minimum.

Emails and Internet Usage

Confidential information must never be sent via external email, either as part of the message or attached as a Word, Excel or other document, which contains personal information about service users or staff, unless the email is encrypted at both ends of the communication or is password protected using an agreed standard. Emails sent to and from health and social care organisations must meet the secure email standard (DCB1596) so that everyone can be sure that sensitive and confidential information is kept secure. You can find out more about the standard, and the action you must take at 'The secure email standard,' NHS Digital.

One of the largest risks with email is misdirection as a result of human error. Where possible, copy and paste the email address from a recorded source to avoid mis-typing the email address. When

communicating sensitive information, a test email should always be sent first, with the information only provided once the recipient has confirmed receipt of the test email. Take your time when emailing personal information, pause and check the email address, email trail and any attachments, and ensure no one other than the recipient has accidentally been included in the 'to' or 'cc' fields. If you are unsure you should check if the recipient's email address is secure and that they know the nature of the information being transmitted.

Data Security and Protection Toolkit

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. You can find out more about the toolkit at 'Data Security and Protection Toolkit', NHS Digital.

Care should be taken to practice good data security when transmitting personal, sensitive or confidential information.

Digitising Social Care

Digital Social Care work in partnership with NHS Digital to support adult social care providers to support their digital transformation. They have a range of free supported resources and guidance which can be accessed at 'Digitising Social Care.'

You can also find useful information and resources at the 'Digital Care Hub' (the new name for Digital Social Care).

The company's standard disclaimer should always be in evidence on emails sent by you.

You should not breach any copyright or intellectual information when transmitting information.

You should not send any inappropriate material to any party which could be deemed to be offensive, abusive, obscene, discriminatory, harassing, defamatory or derogatory, whether or not the recipient indicates they would not object. If you receive any transmission which you deem to be offensive or upsetting, you should immediately notify your Line Manager.

Additionally, you should not:

- Use the system for personal use
- Send or forward chain mail, junk mail, jokes, gossip etc.

- Use the system for trivial and unnecessary messages

You must not visit any site or download any information which is illegal, immoral, offensive, abusive, obscene, discriminatory, harassing, defamatory or derogatory. If you have reason to believe a member of staff of doing so, you should report your concerns to your Line Manager as soon as possible.

You should not attempt to access any information which you know is restricted and you are not authorised to view.

Personal use of our internet system is forbidden.

We reserve the right to intercept and read all emails and attachments sent via the company email and internet system and/or using a company email address provided to a staff member.

The organisation will monitor the use of our email and internet system, including where appropriate opening and reading emails (in line with Data Protection legislation). It is therefore important that you do not send any personal emails, particularly of a sensitive or embarrassing nature.

We will monitor usage to ensure:

- Company policies, standards and guidelines are being followed
- To provide evidence of transmissions and communication
- To ensure there is no unauthorised usage

Inappropriate use of the company email and internet system, e.g. sending pornography or other offensive material, will lead to disciplinary action in line with our 'Disciplinary Policy.' Depending on the severity of the circumstances, it could lead to your summary dismissal.

Social Media, Service Users, Their Family and Staff

Managers and staff are required to follow the appropriate codes of conduct at all times relevant to their professional and work groups, which for this organisation includes:

- Skills for Care: Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in England

The Code of Conduct sets out the required behaviour and professional boundaries expected of staff when working for the organisation and delivering services to adults at risk within the community.

Section 5 of the code provides guidance for staff on 'Respecting People's Right to confidentiality' and states:

- treat all information about people who use health and care services and their carers as confidential.
- only discuss or disclose information about people who use health and care services and their carers in accordance with legislation and agreed ways of working.
- always seek guidance from a senior member of staff regarding any information or issues that you are concerned about.
- always discuss issues of disclosure with a senior member of staff.

Breaching professional boundaries and/or this policy could have consequences from a safeguarding perspective, could lead to allegations of abuse and could lead to staff being disciplined through our 'Disciplinary Policy.'

In addition, staff must not share personal information about other staff or confidential information about the company on any social media platform or other communication service that could bring them, their colleagues or the organisation into disrepute, or which is personal information and/or breaches the Data Protection Act 2018 (See also our 'Social Media Policy').

Nurses, Nursing Associates

Respect people's right to privacy and confidentiality as in the Nursing and Midwifery Code of Professional Conduct.

As a nurse, midwife or nursing associate, you owe a duty of confidentiality to all those who are receiving care. This includes making sure that they are informed about their care and that information about them is shared appropriately.

To achieve this, you must:

- Respect a person's right to privacy in all aspects of their care.
- Make sure that service users are informed about how and why information is used and shared by those who will be providing care.
- Respect that a person's right to privacy and confidentiality continues after they have died – see the 'End of Life Policy.'
- Share necessary information with other health and care professionals and agencies only when the interests of patient safety and public protection override the need for confidentiality.
- Share with service users, their families and their carers, as far as the law allows, the information they want or need to know about their health, care and ongoing treatment sensitively and in a way they can understand.

Breaches of This Policy

Breaches of the confidentiality policy could lead to disciplinary action in line with our 'Disciplinary Policy.' Depending on the severity of the circumstances, it could lead to your summary dismissal.

References and Further Reading

Professional standards of practice and behaviour for nurses, midwives and nursing associates, NMC

Code of Conduct for Healthcare Support Workers and Adult Social Care Workers in England, Skills for Care

Data Protection

Subject Access Request, ICO

Data Sharing Code of Practice, ICO

Information Sharing Policy, NHS

Special Category Data, ICO

Confidentiality Policy 2019, NHS

The secure email standard, NHS Digital

Data Security and Protection Toolkit

Digital Care Hub

Digital Care Hub Resources

Data Security and Protection Toolkit, NHS

Digitising Social Care

Information sharing in social care, NHS Transformation Directorate

Key principles of confidentiality, HCPC

Safeguarding adults: sharing information, SCIE

A Guide to Confidentiality in Health and Social Care, NHS Digital

Privacy and dignity in care, SCIE

Quality Statements

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.

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.

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 1

Confidentiality Do's and Don'ts (Cited from the 'NHS England and NHS Improvement Confidentiality Policy')

Do's

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of NHS England or NHS Improvement.

- Do clear your desk at the end of each day, keeping all non-digital records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer person-identifiable or confidential information securely when necessary, i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain, e.g. gov.uk.
- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken.
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.