Kinwood care limited - Management

Data Protection, Information Governance, CCTV & GDPR Policy Residential

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

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 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.

The organisation is registered with the Information Commissioners Office (ICO) ZB955182.

Please see ‘ICO - Contact us.’

This policy and procedure are provided for the regulated activity of accommodation for people with personal care or nursing.

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

- 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.
- We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default. This policy includes in its scope all data which we process either in hardcopy or digital copy; this includes special categories of data.
- We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the UK General Data Protection Regulation, and all other relevant legislation.
- The Caldicott Principles are embedded within the organisation to ensure confidentiality and the sharing of information to promote safe and effective care provision.
- Caldicott Guardians are senior people within an organisation who protect the confidentiality of people's information by considering the ethical and legal aspects of data sharing. Previously only NHS and local authority bodies were required to have a Caldicott Guardian. Guidance issued in August 2021 requires adult social care services who provide a publicly funded service to appoint a Caldicott Guardian.
- All staff are required to read and comply with this policy, and any breach of the policy may be deemed as gross misconduct and be managed under the organisation's disciplinary policies.
- The organisation will use resources including ICO and Digital Social Care to ensure policies and procedures are updated in line with the latest legislation, regulations, and guidance to ensure resident and staff data is secure and well managed.
- All CQC registered care providers should complete the Data Security and Protection Toolkit (DSPT) at least once a year (see references). It is also a requirement to submit the toolkit if you deliver services under a NHS contract, use a shared health and care record, or are applying for NHSMail. The DSPT has an annual deadline for completion every year. Please see 'Better Security, Better Care, Digital Care Hub' for further information on the annual completion date requirements and supportive resources.

Policy Statement

This policy must be read and implemented by all staff, managers and directors of the organisation.

The organisation has 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, to keep people we support safe, and deliver a caring, responsive, effective and well-led service.

The Policy

This ‘Data Protection Policy’ is the overarching policy for data security and protection for **Kinwood care Limited** (hereafter referred to as ‘us,’ ‘we,’ or ‘our’).

Principles

- We are registered with ICO and use its guides to legislation to support the organisation’s practice in data management, security and record keeping.
- We will be open and transparent with residents and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.
- We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the UK General Data Protection Regulation, and all other relevant legislation.
- We will establish and maintain policies for the controlled and appropriate sharing of people we support's and staff information with other agencies, taking into account all relevant legislation and citizen consent.
- Where consent is required for the processing of personal data, we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our ‘Record Keeping Policy: Withdrawal of Consent’ procedures. We ensure that it is as easy to withdraw consent as it is to give it.
- We will undertake annual audits of our compliance with legal requirements.

Data Protection Act 2018

We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).
- Accurate and kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’).
- Processed in a manner that ensures appropriate security of the personal data.

UK GDPR

We uphold the personal data rights outlined in the UK GDPR:

- The right to be informed
- The right of access
- The right to rectification

- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Due to our size, we have determined that we are not required to have a Data Protection Officer (DPO), as we do not process special categories of data on a large scale. Nonetheless, to ensure that every individual's data rights are respected and that there are the highest levels of data security and protection in our organisation, we have appointed a member of staff to the Data Protection Champion role. The Data Protection Champion will report to the highest management level of the organisation. We will support the Data Protection Champion with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

Underpinning Policies and Procedures

This policy is underpinned by the following:

- Data Quality Policy – outlines procedures to ensure the accuracy of records and the correction of errors.
- Record Keeping Policy – details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share.
- Data Security Policy – outlines procedures for ensuring the security of data including the reporting of any data security breach.
- Network Security Policy – outlines procedures for securing our network
- Business Continuity Policy –outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day-to-day running of our organisation.
- Staff Data Security Code of Conduct - provides staff with clear guidance on the disclosure of personal information.
- Surveillance Equipment & CCTV Policy – sets out the safe procedures and principles for considering and using CCTV and other surveillance equipment.

Data Protection By Design and By Default

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist:

- All new systems used for data processing will have data protection built in from the beginning of the system change.
- All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.
- We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.
- In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for, and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.
- Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

Responsibilities

Our designated Data Protection Champion is Chris Storer. The key responsibilities of the lead are:

- To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles.
- To define our data protection policy and procedures and all related policies, procedures, and processes and to ensure that sufficient resources are provided to support the policy requirements.
- To complete the 'Data Security & Protection Toolkit' (DSPT) annually and to maintain compliance with the DPST.
- To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management and DPO to fulfil this work.

.

Our Senior Information Risk Owner (SIRO) is Chris Storer. The key responsibilities of the SIRO are: To manage, assess and mitigate the information risks within our organisation. To represent all aspects of information and data protection and security to senior management and drive engagement in data protection at the highest levels of the organisation.

Surveillance Technology

Surveillance technology includes CCTV, cameras and microphones. It can help you keep people safe and monitor their care. If you use it, it is important that you do it in a way that protects people's privacy and human rights.

Surveillance technology can help you:

- Protect people's safety, for example from the risk of unsafe care or treatment.
- Keep premises and property secure.
- To help people stay safe without restricting their activities.

Overt surveillance

Before using overt surveillance such as CCTV, we will speak to people this may affect, gain consent where this is required and/or put-up clear notices such as posters. Using surveillance to help keep people safe or monitor their well-being, such as telecare, forms part of their care and must meet the regulations under the Health and Social Care Act. Any recordings you make of people also count as information about them.

Covert surveillance

Before using covert surveillance (using hidden cameras or microphones people are not aware of) we must seek legal advice. This is only likely to be appropriate in very rare circumstances. For example, to identify a specific incident or allegation. Legal advice would need to be obtained to help us decide whether to use covert surveillance.

Before using any type of surveillance staff must:

- Identify the purpose of the surveillance.
- Check that surveillance is the best way of achieving your goal.
- Identify that the surveillance is necessary and proportionate
- Involve the resident/representatives in deciding how it is used

Consider the following factors:

- If there an alternative option that would intrude less on people's privacy?
- Is it the best use of resources?
- Have you checked The General Data Protection Regulation (UK GDPR), this regulation is about data protection and privacy, and Article 8 of the Human Rights Act 1998 which sets out people’s right to privacy to ensure your actions are lawful?

Remember - using surveillance involves processing data about people. You must process data in a way that is lawful, fair and transparent.

Keep a record of your rationale for using surveillance:

- The purpose for using surveillance, including how it supports people's needs.
- The initial assessment.
- The alternatives to surveillance you have considered.

Staff must also keep ongoing records showing:

- Who is responsible for operating the surveillance system.
- How you protect and manage the information it collects.

You must make sure the only people with access to recorded information are people with a legitimate and lawful need. For example:

- CCTV monitors need to be in a lockable office.
- You must use strong passwords to protect information.

Please note: the information presented on surveillance includes guidance provided by 'CQC - Using surveillance in your care service' including the importance of following: The National Data Guardian's 10 standards, set out in the National Data Guardian's 'Review of data security, consent and opt out's.'

Caldicott

The overarching aim of the organisation is to ensure that there is an appropriate balance between the protection of the resident's information, and the use and sharing of such information to improve care.

All staff will be trained through information governance training on the Caldicott Principles and how these support the Data Protection Act 2018 and UK GDPR.

Staff are required to incorporate the following principles within their practice, and managers will through training, supervision, and appraisal ensure that staff are competent in data protection, UK GDPR and the Caldicott Principles.

Appointing a Caldicott Guardian

Caldicott Guardians are senior people within an organisation who protect the confidentiality of people's information by considering the ethical and legal aspects of data sharing. Previously only NHS and local authority bodies were required to have a Caldicott Guardian. Guidance issued in

August 2021 requires adult social care services who provide a publicly funded service to appoint a Caldicott Guardian by June 2023. It may not be feasible or proportionate for some organisations to have a Caldicott Guardian. Some organisations may choose to share a Caldicott Guardian. Some organisations may agree with a commissioner that they will access the commissioning organisation Caldicott Guardian for advice whenever necessary. The National Data Guardian (NDG) has provided guidance on the appointment of Caldicott Guardians.

- NDG - Guidance about the appointment of Caldicott Guardians

All Caldicott Guardians need to be registered on the Caldicott Guardian's registered which is maintained by NHS digital.

- The Eight Caldicott Principles, National Data Guardian

Principle 1: Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and residents.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and residents within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and residents about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

References and Further Reading

Please note: this policy has been adapted from the Digital Care Hub Data Protection policy template

The Data Protection Act 2018

Data Protection and Security Toolkit, NHS

Handling personal information, CQC

Information Commissioner's Office

Digital Social Care

Data Protection Impact Assessment, ICO

Data Sharing Template, Digital Care Hub

A guide to good practice for digital and data-driven health technologies

Data Security and Protection Toolkit Key roles and the DPO, NHS

Using surveillance in your care service, CQC

Data Security and Protection Responsibilities, Digital Social Care

The Eight Caldicott Principles, National Data Guardian

Caldicott-guardians-what-social-care-providers-need-to know, Digitising Social Care

Better Security, Better Care, Digital Care Hub

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