Angels Healthcare LTD

Data Protection, Information Governance, CCTV & GDPR Policy

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

17

Key Lines of Enquiry

W1.4

Scope

In the organisation's day to day delivery of services it is required to use and manage service user, staff and other personal data to ensure the delivery of services in line with the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014. The data is required to ensure the delivery of a safe, caring, responsive, effective and well-led service. This policy will ensure the organisation's management of personal information will comply with the relevant legislation including General Data Protection Regulations (2016) and the Data Protection Act 2018.

The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection. 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) and our registration number is n/a.

ICO Contact details: https://ico.org.uk/global/contact-us/ (https://ico.org.uk/global/contact-us/)

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

- 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 General Data Protection Regulation and all other relevant legislation.
- 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 service user and staff data is secure and well managed.

Policy Statement

This Data Protection Policy is the overarching policy for data security and protection for Angels healthcare ltd (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 service users 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 General Data Protection Regulation and all other relevant legislation.
- We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking 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 na annual audits of our compliance with legal requirements.

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 is processed ('storage limitation').
- Processed in a manner that ensures appropriate security of the personal data.

We uphold the personal data rights outlined in the 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.

Check here to decide if you require a Data Protection Officer (DPO) then select one of the following paragraphs below and delete this text. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/#ib1 (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/#ib1)]

If you decide that you require a DPO your text is:

In line with legislation, we employ a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

If you decide that you do not require a DPO your text is:

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 is 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.

NB: You should make sure that there is somebody who is responsible for data security and protection within your organisation, though you do not have to call them a Data Protection Champion.

Underpinning Policies & 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 the ensuring the security of data including the reporting of any data security breach.
- 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.

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 individuals' 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:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/).

- 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 Jill church . 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 DSPT.

https://www.dsptoolkit.nhs.uk/ (https://www.dsptoolkit.nhs.uk/)

- 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.

JILL church

jill church

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 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 cover 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.

Consider the following factors:

- If there an alternative option that would intrude less on people's privacy?
- Is it best use of resources?
- Have you checked The General Data Protection Regulation (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 at:

- https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service (https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service)

Please note: this policy has been adapted from the Digital Social Care Template Policy at:

- https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/ (https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/)

Policy Review

Policies are reviewed annually or sooner if required.

Name:

Role:

Date Policy Reviewed & Signed Off:

Next Policy Review Date:

Responsible Person:

References and Further Reading

The Data Protection Act 2018

- https://www.gov.uk/data-protection (https://www.gov.uk/data-protection)

Data Protection and Security Toolkit

- https://www.dsptoolkit.nhs.uk/ (https://www.dsptoolkit.nhs.uk/)

CQC Handling personal information

- https://www.cqc.org.uk/guidance-providers/all-services/check-way-you-handle-personal-information-meets-right-standards-0 (https://www.cqc.org.uk/guidance-providers/all-services/check-way-you-handle-personal-information-meets-right-standards-0)

Information Commissioners Office

- https://ico.org.uk/ (https://ico.org.uk/)

Digital Social Care

- https://www.digitalsocialcare.co.uk/ (https://www.digitalsocialcare.co.uk/)

Digital Social Care: Template Policies

- https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/ (https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/)

Data protection impact assessments, ICO

- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)

NHS Data Sharing Template

- https://www.nhsx.nhs.uk/media/documents/Template_Data_Sharing_Agreement_-_MASTER_1.docx (https://www.nhsx.nhs.uk/media/documents/Template_Data_Sharing_Agreement_-_MASTER_1.docx)

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

- https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology#principle-1-understand-users-their-needs-and-the-context (https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology#principle-1-understand-users-their-needs-and-the-context)

Data Security and Protection Toolkit Key roles and the DPO

- https://www.dsptoolkit.nhs.uk/Help/Attachment/61 (https://www.dsptoolkit.nhs.uk/Help/Attachment/61)

Using surveillance in your care service, CQC

- https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service (https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service)

Data Security and Protection Responsibilities, Digital Social Care

- https://www.digitalsocialcare.co.uk/wp-content/uploads/2019/04/3.-Data-Security-and-Protection-Responsibilities-v7.pdf (https://www.digitalsocialcare.co.uk/wp-content/uploads/2019/04/3.-Data-Security-and-Protection-Responsibilities-v7.pdf)

Data Security and Protection Toolkit: 'Entry Level' Guidance for Social Care Providers.

- https://www.digitalsocialcare.co.uk/wp-content/uploads/2019/08/DSPTEntryLevelGuideASC_v8.pdf (https://www.digitalsocialcare.co.uk/wp-content/uploads/2019/08/DSPTEntryLevelGuideASC_v8.pdf)