Service Management

Data Protection: General Data Protection Regulation (GDPR)

Purpose

To comply with the Data Protection Bill, the General Data Protection Regulation (GDPR), and the Freedom of Information Act 2000.

To ensure that individual's rights concerning their personal data and the processing of that data are protected.

To ensure that everyone who deals with personal and sensitive data understands their responsibilities and does not breach confidentiality.

Definitions

Data Subject

The living individual who is the subject of the data/personal information.

Personal Data

Any information that can be used to directly or indirectly identify the 'data subject'. This includes but is not limited to;

- identification numbers.
- IP addresses.
- CCTV footage etc.

Sensitive Personal Data

- Racial or ethnic origin.
- Political opinion.
- Religious beliefs or other beliefs of a similar nature.
- Physical or mental health condition.
- Sexual orientation or behaviour.
- The commission, or alleged commission, of any offence, or any court proceedings or sentence relating to any offence committed or alleged to have been committed.

Processing

Processing pertains to any operation performed on personal data. This constitutes any action like collecting, storing, using, sending, or deleting personal data. Collecting includes recording, and using includes retrieval, modification, combining, linking data, analysing and comparing data.

Data Controller

A person or organisation that determines the purposes for which, and the manner in which, personal information is to be processed. Data controllers are responsible for the compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

Data Processor

A person who processes personal information on a data controller's behalf. Anyone responsible for the disposal of confidential waste is also included under this definition.

Informational Privacy

The ability of a person to control, edit, manage and delete information about themselves and to decide how, and to what extent, such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through surveillance or through the monitoring of communications whether by post, phone or online, and extends to monitoring the records of senders and recipients as well as the content of messages. It also includes the taking of biometric information.

Policy Statement

PENNY POT CARE HOME is responsible for substantial amounts of personal and sensitive data given to it by individuals and other organisations. Every care is taken to protect personal data and to avoid a data protection breach. However, in an event of data being lost or shared inappropriately, it is imperative that the appropriate action is taken to minimise any associated risk as soon as possible.

The Data Protection Bill requires every data controller who is processing personal information to register with the Information Commissioners Office (ICO).

PENNY POT CARE HOME has a certificate of registration that is renewed annually.

"Every citizen should feel confident that information about their health is securely safeguarded and shared appropriately when that is in their interest. Everyone working in the health and social care system should see information governance as part of their responsibility."

F. Caldicott 2013

A review was commissioned in 1997 by the Chief Medical Officer of England, "owing to increasing concern about the ways in which patient information is being used in the NHS in England and Wales and the need to ensure that confidentiality is not undermined. Such concern was largely due to the development of information technology in the service, and its capacity to disseminate information about patients rapidly and extensively".

A committee was established under the chairmanship of Dame Fiona Caldicott and its findings were published in December 1997.

The Caldicott Report highlighted six key principles, and made 16 specific recommendations.

In 2012 Dame Caldicott produced a follow up report which made 26 further recommendations including the addition of a seventh principle which is included in the list below.

The Caldicott Principles (For Service Users)

1. **Justify the purpose(s)**
   Every single proposed use or transfer of Service User identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use Service User's identifiable information unless it is necessary**
   Service User identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for Service User to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary Service User identifiable information**
   Where use of Service User identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
4. **Access to Service User identifiable information should be on a strict need-to-know basis**
   Only those individuals who need access to Service User identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
5. **Everyone with access to Service User identifiable information should be aware of their responsibilities**
   Action should be taken to ensure that those handling Service User identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect Service User confidentiality.
6. **Understand and comply with the law**
   Every use of Service User identifiable information must be lawful. Someone in each organisation handling Service User information should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect Service User confidentiality**
   Professionals should, in the Service User's interest, share information within this framework. Official policies should support them in doing so.

PENNY POT CARE HOME will comply with these principles to ensure that confidentiality is not undermined.

Any information shared or received will be documented to allow an information audit.

Information Governance

GDPR Principles

Personal Data should be:

1. **Processed lawfully, fairly and in a transparent manner**
   Lawfully – processing must be done in line with the requirements within the legislation, and any regulatory or contractual requirements, and any duty of confidentiality.
   Fairly – there must be a legitimate reason for collecting and using the data, be transparent about how the data is to be used, handle the data in a way that would be reasonably expected and not use in ways which would have an adverse effect on the individual.
2. **Collected for specific, explicit and legitimate purposes**
   This is to ensure that the reasons for obtaining personal data are obvious and that what is done with the information is in line with the reasonable expectations of the individuals concerned. If an organisation intends to use the data they hold for other purposes than for what it was collected, they should inform the individuals concerned.
3. **Adequate, relevant and limited to what is necessary**
   Adequate – having enough information to fulfil the purpose(s) for which it was obtained.
   Relevant – justification is on a case by case basis.
   Not excessive – data minimisation – consideration should be given to the type of data collected, how much is held, and how long it should be retained.
4. **Accurate and, where necessary, kept up to date**
   Accurate – data will be inaccurate if it is incorrect or misleading as to any 'matter of fact'. Data must be kept up to date - however may become inaccurate over time. There is some expectation on individuals to inform the organisation when information held has changed. Opinions about individuals are personal data. However, generally, opinions cannot be challenged under the 4th principle. Opinions should be recorded as such and put in context where appropriate.
5. **Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which those data are processed**
   There are statutory requirements to retain some information and those guidelines should be followed. The 5th principle is there to prevent retention of personal data without good reason. Any deletion of personal information must be done securely.
6. **Processed in a manner that ensures appropriate security of the personal data**
   Personal data must be processed in line with the data subject's rights:

   - The right to know who will see and use their personal data.
   - The right to know why their data is being collected and what it will be used for.
   - The right to have copies of ALL their personal data that is being processed or held.
   - The right to have any codes or jargon within provided copies of their personal data explained to them.

7. **Personal Information must be secure**
   There ought to be appropriate and organisational measures in place to protect the personal data that is handled.

Rights for individuals under GDPR

- Subject access.
- To have inaccuracies corrected.
- To have information erased.
- To prevent direct marketing.
- To prevent automated decision-making and profiling.
- Data portability.

Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) can help to identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy.

Privacy Risk

The risk of harm arising through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- Inaccurate, insufficient, or out of date
- Excessive or irrelevant
- Kept for too long
- Disclosed to individuals without consent from, or knowledge of, the data subject
- Used in ways that are unacceptable to, or unexpected by, the data subject
- Not kept securely

The outcome of a DPIA should be a minimisation of privacy risk.

The DPIA includes the following steps:

- Identification for the need to have a DPIA
- Describes how information flows
- Identifies the privacy and related risks
- Identifies and evaluates the privacy solutions
- Records the DPIA outcomes
- Integrates the outcomes into a project plan
- Has consulted with internal and external stakeholders as needed throughout the process

The Data Protection Impact Assessment has been conducted and is held in the Managers Office.

For more information visit: https://ico.org.uk/media/for-orgainsations/documents/1595/pia-code-of-practice.pdf.

Privacy Statement

This privacy notice sets out how we collect and use your personal data.

We respect privacy, and only collect and process your data in accordance with the UK data protection legislation currently in force.

We are registered as a Data Controller with the UK Information Commissioner's Office (ICO).

Our Data Protection Registration Number is Z1048363.

Data regarding service user is collected and stored to ensure an optimum level of care is delivered by suitably trained and qualified staff, with the correct skill mix and in sufficient numbers, to service

user's that have consented to sufficient data being collected about them in order to assist receiving the appropriate care and treatment.

Data regarding employees is collected and stored for employment regulatory reasons i.e. CQC and HMRC.

Data regarding service user's advocates is collected and stored to ensure advocates are kept informed of service users health, care, legal and general needs.

Data will only be stored securely for the regulatory period of time (see retention policy) and will only be shared with other professionals for which consent has been obtained.

Data that is stored can be reviewed and corrected at any time.

Procedure

Consent will be obtained from all individuals for the collection of their personal data and for the purpose in question. Where an individual lacks capacity then the principles of the Mental Capacity Act 2005 will be followed.

All records and documents that contain personal data for all individuals and staff will be kept securely, and personal data will only be accessed by authorised personnel for legally authorised purposes.

The lockable security arrangements will also protect the personal data against accidental or unlawful destruction, accidental loss or alteration, unlawful storage, processing, access or disclosure.

All personal data will be accurate and up to date.

All personal data will be deleted or destroyed as soon as there is no further need for it.

All confidential paper waste is to be shredded.

The premises will also be physically secure and the Security Policy and Procedure followed.

CareDocs computer security:

- All data stored on the server computer system will be encrypted.

- Computers will have a firewall and virus checking system installed.
- The operating system will be set up to receive automatic updates.
- The latest patches and security updates will be downloaded to cover vulnerabilities.
- Staff will only be allowed access to the information that they need to do their job, and must not share passwords.
- Regular back-ups of the information on the computer system will be made and stored in its encrypted format on USB flash drives, in a separate place so that if the computer is stolen or damaged, the information is not lost.
- Computers must not be left unattended if logged onto any personal data system.

Information will not be disclosed to a third party without the express permission of the person who is the subject of the data.

Personal data will not be disclosed over the telephone unless it has been established as a valid contact point e.g. health or local authority; regulatory body.

Staff must use strong passwords that are long (at least eight characters), have a combination of upper and lower-case letters, numbers, and special keyboard characters.

Staff will receive training concerning Data Protection and in particular the introduction of GDPR.

Staff must understand that breaches of data protection and confidentiality will be considered as gross misconduct and will carry the appropriate penalty which may also incur legal prosecution.

Any breach of data protection and confidentiality must be reported to the data controller immediately.

If a breach of security has occurred i.e. the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data – notification within 72 hours must be made to the supervisory authority. The notification will contain information as to whether there is likely to be significant detrimental effect on individuals.

Subject Access Requests (SARs)

A Subject Access Request (SAR) is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under section 7 of the Data Protection Act 1998. The request does not have to be in any particular form, nor does it have to include the words 'subject access' or make any reference to the Data Protection Act. Indeed, a request may be a valid SAR even if it refers to other legislation, such as the Freedom of Information Act.

A SAR must be made in writing. An emailed or faxed request is as valid as one sent in hard copy.

Proof of identity is required so that the data controller can verify who is making the request.

Requesters do not have to state their reason for making the request, or what they intend to do with the information requested.

The SAR will be responded to within one month.

There will be no administration fees charged.

Third Parties

When providing information that includes a third party, a case by case decision will be made as to whether to provide the information.

Consideration will be given to deleting names or editing documents that would identify a third person if that person has not consented to being identified.

More information can be obtained from https://ico.org.uk.

The Information Commissioners Office (ICO) and the Care Quality Commission (CQC) have issued guidance on the use of surveillance. However, under the Data Protection Act the following principles apply.

The guiding principles of the Surveillance Camera Code of Practice

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose, and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.