Data Protection and Compliance with the General Data Protection Regulation (England) Policy

Aim and Scope of Policy

The policy, which is in line with UK data protection laws, shows how this care service complies with the data protection requirements found in Regulation 17: "Good Governance", of the Health and Social Care Act (Regulated Activities) Regulations 2014.

To comply with these regulations the care provider must have good governance of record keeping resulting in records that are comprehensively fit for purpose and securely maintained.

The care provider recognises that it must keep full, accurate, up-to-date records on people receiving care, staff and other aspects concerning the running of the service in line with data protection, confidentiality, secure storage and authorised access policies and procedures.

This care provider also understands that all records required for the protection of people receiving care and for the effective and efficient running of the care service should be collected, maintained and kept according to the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

This data protection policy applies to all manual and digital records kept by the service in relation to people receiving care, including those involved with them, whose personal data might be found on their records. This includes all staff and any third parties (agencies and professionals) with whom anyone's personal data information held by the service might have to be disclosed or shared.

The policy is used with other relevant record-keeping and information governance policies.

Policy Statement

The care service recognises it must keep all records required for the protection and wellbeing of people receiving care, and those for the effective and efficient running of the care service such as staff records to comply currently with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), which came into force in May 2018.

In line with its registration under the Data Protection Act, and to comply with GDPR, the service understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

This means that all personal data obtained and held by the care service to carry out its activities as a registered care provider must:

- have been obtained fairly and lawfully
- held for specified and lawful purposes as an organisation that is carrying out a public duty
- processed in recognition of persons' data protection rights, which are described in GDPR in terms of the right:
  - to be informed
  - to have access
  - for the information to be accurate and for any inaccuracies to be corrected
  - to have information deleted (eg if inaccurate or inappropriately included)
  - to restrict the processing of the data to keep it fit for its purpose only
  - to have the information sent elsewhere as requested or consented to (eg in any transfer situation)
  - to object to the inclusion of any information (eg if considered to be irrelevant)
  - to regulate any automated decision-making and profiling of one's personal data
- be adequate, relevant and not excessive in relation to the purpose for which it is being used
- be kept accurate and up to date, using whatever recording means are used or agreed (eg manual or electronic)
- not be kept for longer than is necessary for its given purpose (eg in line with agreed retention protocols for each type of record)
- have appropriate safeguards against unauthorised use, loss or damage with clear procedures for investigating any breaches of the data security
- comply with the relevant GDPR procedures for international transferring of personal data.

In line with the Data Protection Act 2018 and the GDPR, the care service has a data controller and a nominated data protection officer, who is responsible for the safekeeping and safeguarding of all personal data held by the care service.

Procedures

The service has taken the following steps to protect everyone's personal data, which it holds or to which it has access so that it complies with current data protection laws and GDPR.

1. It appoints or employs staff with specific responsibilities for:

a. the processing and controlling of data (data controller)

b. the comprehensive reviewing and auditing of its data protection systems and procedures (data protection manager or auditor)

c. overviewing the effectiveness and integrity of all the data that must be protected (data protection officer).

There are clear lines of responsibility and accountability for these different roles.

2. It provides information to people who use services and others involved in their care on their data protection rights, national data opt-out policy, how it uses their personal data and how it protects it. The information includes the actions people who use services and staff can take if they think that their data has been compromised in any way (eg through the complaints procedure or grievance procedure in the case of staff).

3. It provides its staff with information and training to make them aware of the importance of protecting people's personal data, to teach them how to do this, and to understand how to treat information confidentially.

4. It can account for all personal data it holds, where it comes from, and who it is and might be shared with.

5. It carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the service.

6. It recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions.

7. It has policies and procedures for enabling people who use services and/or staff to have access to their personal information, and for the making of subject access requests that are in line with GDPR.

8. It has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences (eg fine).

Compliance With Data Protection Law and the GDPR After the End of Covid-19 Restrictions

The care service has followed the advice and guidance of the Information Commissioner's Office during the Covid-19 restrictions. Since these have been lifted the care provider will continue to follow ICO updated advice to the effect.

1. It has reviewed all extra personal information collected during the pandemic for its current lawfulness, purpose and usefulness and taken steps to dispose anything that is no longer needed.

2. In doing so the care service follows current government guidance on what information is still required or might need to be shared on public health grounds.

3. It will continue to submit data to the DHSC Capacity Tracker as required by the provisions of the Health and Social Care Act 2022, which requires information on the vaccination status of care staff.

4. The care provider understands that this and any other information that qualifies as personal information can only be obtained and submitted with each person's full consent.

5. The care provider recognises that with any such requests for information it must only provide it if there is a lawful and compelling reason for doing so. It will only provide this after it has processed the information fairly.

National Data Opt-Out Policy

All regulated social care providers in England need to comply with the national data opt-out policy by 31 July 2022.

Introduced by the National Data Guardian in the *Review of Data Security, Consent and Opt-Outs* (2018), the national data opt-out provides everyone with the ability to stop health and adult social care organisations sharing confidential patient information for reasons other than direct care and treatment, such as research or planning.

National data opt-out applies where a person is receiving social care provided, arranged or funded, in part or whole, by Local Authorities or the NHS in England. This does not affect individual care provision, where data processing is legally required, the individual has consented to processing or data has been appropriately anonymised.

It only applies when Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 ("Regulation 5 support") is utilised on a legal basis to process confidential patient information where processing would otherwise be a breach of confidentiality.

The term “confidential patient information” is a specific legal term which applies to information about the health of a person who uses services or social care that can identify them.

Training

New staff must read and understand the policies on data protection and confidentiality as part of their induction.

All staff receive training covering basic information about confidentiality, data protection and access to records.

Training in the correct method for entering information in an individual’s records is given to all care staff.

The nominated data controller/auditors/protection officers for the care service are trained appropriately in their roles under GDPR.

All staff who need to use the computer system are trained to protect individual’s private data, to ensure data security, and to understand the consequences to them as individuals and the organisation of any potential lapses and breaches of the service’s policies and procedures.