Compound Healthcare
Quality, reliable nursing agency

Policy Title	Policy number	**Date Implemented or Date of Last Review**	**Date of Next Review**
Data Protection Policy GDPR	D0C - 028	**28/07/2021**	**28/07/2022**

1. POLICY STATEMENT

5.1 Compound Healthcare Ltd is committed to protecting the rights and privacy of our staff, clients, and others, in accordance with the General Data Protection Regulation (GDPR), May 2018.

5.2 The new regulatory environment demands higher transparency and accountability in how our business manages and uses personal data. It also accords stronger rights for individuals in understanding and controlling that use.

5.3 The GDPR contains provisions that the organisation needs to be aware of as data controllers, including provisions intended to enhance the protection of our staff and clients' personal data.

5.4 The GDPR requires us to ensure that our privacy notices are written clearly in a way that staff and clients will understand.

5.5 To comply with its legal obligations as required by the General Data Protection Regulation (GDPR), Compound Healthcare Ltd will adhere to its principles, and ensure that all information about individuals is collected and used fairly, stored safely and securely, and not unlawfully disclosed to any third party.

5.6 The ICO's website (www.ico.gov.uk) provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed, etc. A Guide to Data Protection is available on the website.

2. SCOPE & COMPLIANCE

5.1 'Personal data' is information relating to an individual. This may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

5.2 This policy applies to all staff of Compound Healthcare Ltd. Any breach of this policy or of the Regulation itself is considered to be an offence, and the organisation's disciplinary procedures will be invoked.

5.3 As a matter of best practice, other agencies and individuals working with Compound Healthcare Ltd who have access to personal information are expected to read and comply with this policy.

5.4 This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

3. GENERAL DATA PROTECTION REGULATION (GDPR)

5.1 The GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children).

5.2 The GDPR also sets out specific rights for staff and clients in relation to personal records held within the organisation's system. For example, it gives all individuals who are the subject of personal data a general right of access to the personal data that relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'.

5.3 For more detailed information on these Regulations, see the Data Protection Data Sharing Code of Practice (DPCoP) from the Information Commissioner's Office (ICO) – available on www.ico.gov.uk.

4. RESPONSIBILITIES UNDER THE GDPR

5.1 Compound Healthcare Ltd is the 'data controller' under the terms of the legislation. This means that it is ultimately responsible for controlling the use and processing of the personal data it holds.

5.2 The organisation has appointed a Data Protection Officer (DPO): the director. The DPO is available to address any concerns regarding the data held by the organisation and how it is processed, held, and used.

5.3 The Senior Leadership Team is responsible for all day-to-day data protection matters; for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the organisation.

5.4 The Senior Leadership Team is also responsible for ensuring that the organisation's notification system remains accurate and up to date.

5.5 Compliance with the legislation is the personal responsibility of all members of the organisation who process personal information.

5.6 Individuals who provide personal data to the organisation are responsible for ensuring that the information is accurate and up to date.

5. DATA PROTECTION PRINCIPLES

5.1 The legislation places a responsibility on every data controller to process any personal data in accordance with the seven principles of GDPR.

5.2 The seven principles are that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. ('purpose limitation');

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate regarding the purposes for which they are processed are erased or rectified without delay ('accuracy');

e) Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. ('storage limitation');

f) Processed in a manner that ensures appropriate security of the personal data, with protection, using appropriate technical or organisational measures ('integrity and confidentiality').

g) Processed by data controllers who take responsibility for complying with the principles and have appropriate processes and records in place to demonstrate compliance. ('accountability').

5.3 PROCESSING DATA FAIRLY, LAWFULLY AND TRANSPARENTLY

5.3.1. Compound Healthcare Ltd will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the nature of the data, the purposes of the processing, any disclosures to third parties that are envisaged; they are given an indication of the

period for which the data will be kept, and any other information which may be relevant.

5.4 PURPOSE LIMITATION

5.4.1. Compound Healthcare Ltd will ensure that the specific purpose/s for which it originally collected the data is the only purpose for which it processes the data, unless the individual is informed and consents to any other processing before it takes place.

5.4.2. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be incompatible with the initial purposes.

5.5 DATA MINIMISATION

5.5.1. Compound Healthcare Ltd will ensure that the data is adequate, relevant, and not excessive in relation to the purpose for which it is processed.

5.5.2 Compound Healthcare Ltd will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

5.6 ACCURACY

5.6.1 Compound Healthcare Ltd will keep personal data accurate and up to date.

5.6.2 Compound Healthcare Ltd will review and update all data on a regular basis.

5.6.3 It is the responsibility of the individuals giving their personal data to ensure it is accurate, and they should notify the organisation if, for example, a change in circumstances means that the data needs to be updated.

5.6.4 It is the responsibility of the organisation to ensure that any notification of a change is recorded and acted upon.

5.7 STORAGE LIMITATION

5.7.1 Compound Healthcare Ltd undertakes not to retain personal data for longer than is necessary, to ensure compliance with the legislation and any other statutory requirements.

5.7.2 Personal data may be stored for longer periods, processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by the Regulation to safeguard the rights and freedoms of the data subject.

5.7.3 Compound Healthcare Ltd will undertake a regular review of the information held and implement a process by which only necessary data is retained.

5.7.4 Compound Healthcare Ltd will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding, and disposal of hard copy files as confidential waste). A log will be kept of any records destroyed.

5.8 INTEGRITY AND CONFIDENTIALITY

5.8.1 Compound Healthcare Ltd will process data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5.9 ACCOUNTABILITY

5.9.1 Compound Healthcare Ltd takes responsibility for complying with the principles of GDPR and has appropriate processes and records in place to demonstrate compliance.

6 THE RIGHTS OF THE DATA SUBJECT UNDER THE LEGISLATION

6.1 Individuals have various rights under the legislation including a right to:

a) Be told the nature of the information the organisation holds, and any parties to whom this may be disclosed.

b) Prevent processing likely to cause damage or distress.

c) Prevent processing for purposes of direct marketing.

d) Be informed about the mechanics of any automated decision-making process that will significantly affect them.

e) Not have significant decisions that will affect them taken solely by automated processes.

f) Sue for compensation if they suffer damage by any contravention of the legislation.

g) Act to rectify, block, erase or destroy inaccurate data.

h) Request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

6.2 Compound Healthcare Ltd will only collect, process, or store personal data in accordance with individuals' rights.

7 MEASURES AGAINST UNAUTHORISED/UNLAWFUL PROCESSING AND ACCIDENTAL LOSS/ DESTRUCTION OF DATA

7.1 Compound Healthcare Ltd has put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

7.2 All members of staff are responsible for ensuring that any personal data they hold is kept securely and not disclosed to any unauthorised third parties.

7.3 Compound Healthcare Ltd does not permit personal data or client notes to be taken out of the office or loaded onto laptops. Encrypted systems are used wherever possible.

7.4 Compound Healthcare Ltd will ensure that all personal data is accessible only to those who have a valid reason for using it.

7.5 Compound Healthcare Ltd has appropriate security measures in place, which include:

a. Ensuring that hard copy personal data is kept in locked filing cabinets/cupboards with controlled access (keys are held securely in a separate key cabinet with controlled access).

b. Password-protecting personal data held electronically.

c. Archived personal data is kept securely in locked cabinets.

d. Placing any PCs, terminals, CCTV camera screens, etc. to be visible only to authorised staff.

e. Ensuring that PC screens are not left unattended without a password-protected screensaver being used.

7.6 In addition, Compound Healthcare Ltd has in place appropriate measures for the deletion of personal data. Manual records are shredded or disposed of as 'confidential waste' and appropriate contract terms are in place with third parties undertaking their disposal. Hard drives of redundant PCs are wiped clean before disposal – or if that is not possible, physically destroyed. A log is kept of the records destroyed.

7.7 This policy also applies to staff who process personal data 'off-site', e.g., working at home. Additional care must be taken regarding the security of the data.

8 TRANSFERRING DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

8.1 The organisation will ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

8.2 Compound Healthcare Ltd will not transfer data to such territories without the explicit consent of the individual.

8.3 This also applies to publishing information on the Internet - because data on a website can be accessed from outside the EEA. Compound Healthcare Ltd will always seek the consent of individuals before placing any personal data (including photographs) on its website.

8.4 If the organisation collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website and wherever personal data is collected.

9 CONSENT AS A BASIS FOR PROCESSING

9.1 Although it is not always necessary to gain consent from individuals before processing their data, it is best practice to ensure that data is collected and processed in an open and transparent manner.

9.2 Consent is especially important when Compound Healthcare Ltd is processing any sensitive data, as defined by the legislation.

9.3 Compound Healthcare Ltd understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained based on misleading information will not be a valid basis for processing. Consent cannot be inferred from non-response to a communication.

10 COLLECTION/USE STATEMENT

10.1 Compound Healthcare Ltd will ensure that any forms used to gather data on an individual will contain a 'fair collection statement' explaining the use of that data, how the data may be disclosed and indicate if the individual needs to consent to the processing.

10.2 Such a statement will reference: “For the purposes of the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679, you consent to Compound Healthcare Ltd holding and processing personal data, including sensitive personal data, of which you are the subject; details of which are specified in the organisation's data protection policy. This includes marketing images and the organisation’s CCTV images.”

10.3 Information may be shared with third parties only where the law allows it and when the sharing of such data follows the Data Protection Act 1998.

10.4 Further information about use of, and access to, personal data, and details of organisations with whom we share data is available on request.

10.5 Compound Healthcare Ltd will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, steps will be taken to ensure that the processing of that data does not occur.

11 SUBJECT ACCESS RIGHTS (SARS)

11.1 Individuals have a right to access any personal data relating to them held by the organisation. Any individual wishing to exercise this right should apply in writing to the managing director.

11.2 Under the terms of the legislation, any such requests must be complied with within 40 days.

12 DISCLOSURE OF DATA

12.1 Only disclosures under Compound Healthcare Ltd’s Data Processing notification system must be made. Therefore, staff should exercise caution if asked to disclose personal data held on another individual or third party.

12.2 Compound Healthcare Ltd undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and, in some circumstances, the police.

12.3 Legitimate disclosures may occur in the following instances:

a. the individual has given their consent to the disclosure.

b. the disclosure has been notified to the Information Commissioner’s Office (ICO) and is in the legitimate interests of the organisation.

c. the disclosure is required for the performance of a contract.

12.4 There are other instances when the legislation permits disclosure without the consent of the individual. For detailed guidance on disclosures, see the Code of Practice (CoP).

12.5 Under no circumstances will Compound Healthcare Ltd sell any of its databases, or data therein, to a third party.

13 PUBLICATION OF ORGANISATIONAL INFORMATION

13.1 Compound Healthcare Ltd publishes some organisational data, e.g. internal telephone directory, event information, photos, and information in marketing materials and on its website.

13.2 An individual may wish certain of their data to remain confidential or restricted to organisational access only. Therefore, it is Compound Healthcare Ltd's policy to offer an opportunity to opt-out of the publication of such data when collecting the information.

14 EMAIL

14.1 It is the policy of Compound Healthcare Ltd to ensure that senders and recipients of email are made aware that under the Data Protection Act (DPA), and Freedom of Information legislation, the contents of the email may have to be disclosed in response to a request for information. This will be communicated by a disclaimer on the organisation's email.

14.2 Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the organisation may be accessed by someone other than the recipient, for system management and security purposes.

15 CCTV

15.1 The organisation may install CCTV systems to operate within Compound Healthcare Ltd to protect staff and visitors to our offices. Compound Healthcare Ltd will only process personal data obtained by the CCTV system in compliance with the legislation.

16 PROCEDURE FOR REVIEW

16.1 This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.