**Data Management and Confidentiality Policy**

**1.0 Confidentiality**

1.1 It is a condition of staff employment to treat private information with the utmost confidentiality. Service user information shall not be disclosed to any unauthorised third party outside of the usual list of multi agencies and other external organisations connected to the care/support of the service users without the express consent of the service user, or if the service user is unable to judge the service user's immediate family or advocate.

1.2 The service user shall be kept informed at all times of the outcome of confidential discussions by the care staff and professionals working on the planning and execution of care activities that surround them.

1.3 As per the requirements of our Data Protection Policy, staff involved in the processing of service user’s personal data will take all reasonable precautions to prevent sighting of data by unauthorised persons. Record files are locked away when not in use. It is the policy at 1st Healthcare that the service user has the right to access his/her personal records or Case Notes at any time.

1.4 Care Staff will always consult their immediate Supervisor or Manager if they are unclear with respect to any item concerning confidentiality, or when made privy to confidential information that may have legal and/or criminal connotations e.g. if a service user confides that he/she has allegedly been submitted to sexual abuse by a staff member.

**2.0 Sharing Data**

This covers internal sharing and transmission of service user data or information as well as external sharing and access to service user information with other authorised multi-agencies and the care authorities. External users receive our current data usage compliance and are expected to adhere to the safe process of usage and sharing within their respective organisations.

We require a copy of external users General Data Protection Regulation (GDPR) policy with key parts of the policy which must be identical to our own. Transmission of data to an external party needs to be sent over a secure connection and data needs to be encrypted in the transfer process. Users are able to use the secure pathways from the care management system to share service user reports and documents which contains its own robust security measures competent enough to deal with any form of breach or data loss.

Data shared externally outside our internal database system by email mostly, is done so following strict user guidelines with data security that meets the required standards, the use of password access to emails and or permission protocols recognised in the recipient’s emails.

For internal sharing, most service user details are shared on the database system as reports or caseloads. Staff access the same information using their task permitted username and password to edit or view a report. Staff may receive links to a service user’s data and can only be directed to where the information resides on the system, to access data, the recipient would need to go through the secure login process.

Where the service user has particularly requested certain information to be divulged to a third party. In such cases appropriate notes MUST be made in the service user’s Care Records, together with a signed record of authorisation from the service user or his /her advocate.

Both staff and service users/relatives/advocates will also be advised that personal information held at our Units may be shared with the Registration Authority, as appropriate.

2.1 1st Healthcare shall ensure that all its employees, agents, contractors, or other parties it works adheres to the following when working with personal data:

* All emails containing personal data must be encrypted or password protected prior to issue.
* Personal data that is no longer needed must be erased or otherwise disposed of for any reason
* All Personal data must be securely deleted and disposed of; hard copies should be shredded and electronic copies should be deleted securely.
* Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.
* Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.
* ​Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
* Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.
* Where Personal data is to be transferred in hard copy form it should be passed directly to the recipient or sent using track and recognised mail delivery service such as The Royal Mail
* No personal data may be shared informally and if an employee, agent, sub-contractor, or other third party working on behalf of 1st Healthcare requires access to any personal data that they do not already have access to, such access should be formally requested from the office manager.
* All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar.
* No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of 1st Healthcare or not, without the authorisation of the area manager.
* Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time.
* If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.
* No personal data should be stored on any mobile device including, but not limited to, laptops, tablets and smartphones, whether such device belongs to the Company or otherwise without the formal written approval of the office manager and in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.
* No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of 1st Healthcare where the party in question has agreed to

comply fully with the letter and spirit of this Policy and of the regulation which may include demonstrating to 1st Healthcare that all suitable technical and organisational measures have been taken.

* In cases whereby the service user has particularly requested certain information to be divulged to a third party, appropriate notes MUST be made in the service user’s Care Records, together with a signed record of authorisation from the service user or his/her advocate.
* Both staff and service users / relatives / advocates will also be advised that personal information held at 1st Healthcare units may be shared with the Registration Authority, as appropriate.

2.2 Data portability and access – We recognise our service users rights to access their own care or support information in a physical or digital form. Therefore we will ensure that they are able:

* Move, copy and receive personal data easily from 1st Healthcare’ IT or hard copy archives in a secure and safe and secure way, without affecting its usability.
* Obtain and reuse their personal data for their own purposes across various internal reports and documentation about the details of their care and progression of development covering the duration of their care with 1st Healthcare as their provider.
* Obtain personal information/data in a format that is structured, commonly used and machine - readable.

NB: Access to data applies to information created or managed by 1st Healthcare as a provider and does not include any of their external data accessed from any other external organisation.

**3.0 Internal compliance responsibilities**

We will adhere to the following internal practices:

* All personal data stored electronically should be backed up to the main server with backups stored onsite and offsite.
* All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Company is designed to require passwords.
* Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of 1st Healthcare, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.
* Where personal data held by 1st Healthcare is used for marketing purposes, it shall be the responsibility of sales staff issuing such communications to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least every 6 months.

**4.0 External use compliance**

1st Healthcare shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

* All employees, agents, contractors, or other parties working on behalf of 1st Healthcare shall be made fully aware of both their individual responsibilities and our responsibilities under the regulation and under this policy and shall be provided with a copy of this Policy.
* Only employees, agents, sub-contractors, or other parties working on behalf of 1st Healthcare that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data
* All employees, agents, contractors, or other parties working on behalf of 1st Healthcare handling personal data will be appropriately vetted and trained to do so.
* All employees, agents, contractors, or other parties working on behalf of 1st Healthcare handling personal data will be appropriately supervised.
* Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed.
* The performance of those employees, agents, contractors, or other parties working on behalf of 1st Healthcare handling personal data shall be regularly evaluated and reviewed.
* All employees, agents, contractors, or other parties working on behalf of 1st Healthcare handling personal data will be bound to do so in accordance with the principles of the regulation and this policy by contract.
* All agents, contractors, or other parties working on behalf of 1st Healthcare handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of 1st Healthcare arising out of this Policy and the Regulation.
* Where any agent, contractor or other party working on behalf of 1st Healthcare handling personal data fails in their obligations under this policy that party shall indemnify and hold harmless against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

**5.0 International data transfer**

1st Healthcare may from time to time ‘transfer’ by means of remotely making available personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

* The transfer is to a country, territory, or one or more specific sectors in that country or an international organisation, that the European Commission has determined ensures an adequate level of protection of personal data.
* The transfer is to a country or international organisation which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority e.g. the Information Commissioner’s Office; certification under an approved certification mechanism as provided for in the Regulation; contractual clauses agreed and authorised by the competent supervisory authority.
* The transfer is made with the informed consent of the relevant data subjects.
* The transfer is necessary for the performance of a contract between the data subject and the Company or for pre-contractual steps taken at the request of the data subject.
* The transfer is necessary for important public interest reasons.
* The transfer is necessary for the conduct of legal claims.
* The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
* The transfer is made from a register that, under EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

5.1 Data Breach Notification - All personal data breaches must be reported immediately to the Data Protection Officer (DPO).

5.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage, the staff or manager on site will ensure that the Information Commissioner’s Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

5.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO will ensure that all affected data subjects are informed of the breach directly and without undue delay. Data breach notifications shall include the following information:

* The categories and approximate number of data subjects concerned.
* The categories and approximate number of personal data records concerned.
* The name and contact details of of our DPO or other contact point where more information can be obtained.
* The likely consequences of the breach
* Details of the measures taken, or proposed to be taken, by 1st Healthcare to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

5.4 Modifications to our privacy policy - Aside from the annual reviews /modifications, we may update our privacy policy as and when there is a need such as changes in legislation, mode of practice or compliance. When we change this privacy policy in a significant way, we will send an email or post a notification on our website along with the updated privacy policy to all our account holders/users.

**6. General Data Protection Regulation (GDPR) Compliance**

1st Healthcare has a DPO with dual responsibility to manage the safe and compliant use of data as well as address any data breach or failure issues. The DPO is the link between 1st Healthcare and the external IT services and answerable to internal and external data queries.

1st Healthcare makes use of a bespoke database system which serves as the source of data capture and storage. The database system is managed on rented servers and is used to create, analyze and share information as well as measure outcomes in all areas of care provided. It also serves as a central archive point where previous paper-based reports can be reviewed and updated.

Staff are trained to use the database application safely and ensure data pertaining to each young person in placement is only accessible to authorised individuals with user access settings. Access by external guest users (local authorities /related agencies) also follow strict guidelines on access and sharing protocols in line with the data protection acts and the industry sensitive data protection and usage.

Actual staff usage on the system follows user responsibilities such as safely securing username and password details which are changed on a weekly basis.

Staff are not permitted to work from home and usernames/passwords are locked after office working hours unless a member of staff is on duty at any of the units overnight.

Staff access the records system through approved devices usually no personal devices are to be used to distribute, store or share client data.

**7. Holding data**

All service user’s data are not stored on the internal database indefinitely. When a placement ends, sensitive service user information is transferred to the care authorities with the use of physical storage devices or through the use of encrypted cloud based data transfers. The client data is erased from the system after the stipulated period. Usually after a period of 3 months when all external user access requests have ended. Service users are also informed about this process and are given the option to request copies of the data or hard copy print