HEALTHBOX

COMMUNITY WELLBEING SERVICES

Data Quality & Record Keeping Policy

2021-2022

About this Policy

This policy covers Healthbox CIC's responsibility for the safekeeping of all records from creation to disposal. This also includes our procedures for sharing data externally. This policy covers in it's scope, all data which we process either in hard copy or digital copy, including special categories of data.

Who should read and understand this policy?

All Healthbox CIC staff including full and part time staff, and sessional staff. Depending on role this policy may be relevant to volunteers and placement students or interns.

What is the purpose of this policy?

The availability of accurate and timely data is vital to ensure the safety and the quality of the services we provide. This policy covers:

- ☑ Our record keeping procedure
- ☑ Transparency procedures
- ☑ Procedures for ensuring data accuracy
- ☑ Procedures for correcting errors
- ☑ Retention and disposal procedures
- ☑ Our information handling procedures
- ☑ GDPR subject access requests and rights
- ☑ Our procedure when there is a withdrawal of consent to share

Section 1: Record Keeping Procedure

When we create records, we use standardised structures and layouts for the contents of records.
All records are kept in accessible but protected locations. The location of these records is documented in the Information Asset Register (IAR). The security procedures around access to records are detailed in the Data Security Policy.

Throughout the lifespan of the record we:

- Ensure documentation reflects the accurate records of activity and is viewable in chronological order;

- Provide clearly written session notes, action plans or care plans when support is being delivered by several members of the team, and ensure records are maintained and updated, and shared with those who have a legal basis for seeing the information;

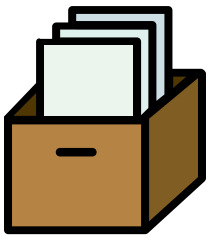
- Provide staff with guidance and training on the creation and use of records and their legal responsibilities to share and safeguard personal confidential information;

- Monitor access to the record. The procedures which detail our auditing and monitoring process are detailed in our **Data Security and Protection Policy**.

- At any point in the lifespan of the record, the data subject has the right to request access to their data. These subject access procedures are detailed in section 7 of this policy.

- At any point in the lifespan of the record, the data subject has the right to request that their record is corrected. These procedures are detailed in the Data Quality Policy.

- At any point in the lifespan of the record, the data subject has the right to request the erasure ('Right to be forgotten') of their record. These procedures are outlined in section 7.



- Records are only retained while they are necessary for the purposes for which they were originally collected. We will ensure that all records are retained and destroyed in-line with our Retention & Disposal Procedures (Section 5).

- At least annually we guarantee that we will audit our record keeping procedures to ensure that they are adequate and continue to keep our records to the highest standards.

Section 2: Transparency Procedures

Our privacy notice outlines to people why we hold their data, the lawful basis for doing so, and their rights in terms of how we process their data.

Our privacy notice is freely available to all individuals whose data we process and is part of our commitment to transparency and accountability. It satisfies the individual's right to be informed under **GDPR.**

Our Privacy Notice and Service User infographic can be found on the Healthbox CIC Website and in our Policies Folder.

All service users, or their legal representative if necessary, will be informed of their rights regarding their personal data when they enrol in Healthbox CIC services.

The privacy notice will be reviewed and updated at least annually.

The privacy notice has been signed off by Senior Management.

We will provide people with this information at the moment that we ask them to give us their personal data.

Section 3: Procedures for Ensuring Data Accuracy

We ensure accuracy in our data in both hardcopy and digital records by making sure all data has the following characteristics:

- **Authentic** – i.e. the data is what is claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed;

- **Reliable** – i.e. the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records;

- **Integrity** – i.e. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified;

- **Useable** – i.e. the data can be located when it is required for use and its context is clear in a contemporaneous* record.

*(occurs at the time or very close to the time of the event)

The principal purpose of service user records is to record and communicate information about the individual and the service they have accessed, including which project or programme and it's impact (Clinical or social impact measures).

The principal purpose of staff records is to record employment details for payroll and business planning purposes.

To fulfil these purposes, we:

- Use standardised structures and layouts for the contents of records; most services use Elemental which allows appointments notes to be recorded alongside baseline and follow-up measures.

- Ensure documentation reflects the continuum of care or service access, that all service delivery is person centred and that records are viewable in chronological order;

- Provide a clearly written service access or action plan when support is being delivered by several members of the team, and we ensure that records are maintained and updated, and shared with everyone involved;

- Train staff on the creation and use of records (see staff handbook) and provide annual training on good record keeping;

- Have implemented a procedure that enables service users and staff to have easy access to their records where appropriate. This is outlined within this policy and our Privacy Notice.

- All staff who record information - whether hardcopy or electronic - **have a contractual responsibility to ensure that the data is accurate and as complete as possible**. This responsibility extends to any system the staff member has access to.

Section 4: Procedures for the Correction of Errors

In-line with national legislation, individuals have the right to have access to their personal data which we process and store. Citizens have the right to **the rectification of said records in the instance that their records are inaccurate or incomplete**.

Where at all possible, in the instance that we have appropriately shared that individual's records with any third-party we will inform this third-party of the rectification if appropriate.

In all cases we will respond to a request for rectification **within one month**. Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why it is required within one month.

To request for their records to be rectified service users or staff should contact us with the request for rectification either verbally or in writing.

Individuals can ask anyone in Healthbox to request this, so staff should know their responsibilities to pass on requests to their Team Manager and directors in a timely manner.

If the rectification is due to the record being incomplete, then the individual should also provide the supplementary information to update the record.

While we are assessing the request to rectify records, we will restrict processing of the data in question. This will be done in line with our Right to Restrict Processing Procedure as outlined in this Policy.

In the instance where the rectification request is refused, the reason will be explained in full and in writing within one month of the original request having been received.

All individuals who have their rectification request refused will be informed of their legal rights to complain to the ICO and to seek a judicial remedy;

All staff will be informed of this policy in the staff handbook.

All service users, or their legal representative, will be informed of this policy, as well as their other rights as regards their personal data, when they sign initial contracts with us.

In order to process a request for rectification, service users might be asked to provide identifying documents so that we can authenticate that it is appropriate to update the data.

Responsibilities

Every member of staff is individually responsible for the quality of data they personally record – whether on paper or electronically. Additionally, they are responsible for reporting any mistakes they do notice to the directors.

Staff are aware that data accuracy and security is a contractual and legislative requirement and that breach of this policy might result in disciplinary action.

Section 5: Retention Schedule & Disposal Procedures

At the end of their lifespan, the records will go through an appraisal process. This process will determine if there is a continuing legal basis for keeping the record. Most records are kept for 2-3 years post project/service completion. Records will not be kept longer than 7 years unless expressly requested by an NHS or Local Authority commissioner. The directors will have final responsibility for determining whether the record will be destroyed or retained. They will maintain a record of all retention or disposal decisions with Team Managers. We will review all project data using a disposal checklist.

In the instance that records are destroyed, our in-house process is:

Paper records:

Paper records will be disposed of using a contracted shredding company. Confidential paper records must be sealed within the supplied shredding disposal bags and locked away in the office until the shredding collection pick-up is made. Keys to the confidential waste bin and documents to securely dispose of locked cabinet are kept in in the combination locked key safe.

Electronic Records:

Projects with scanned enrolment forms or digital participant information will be archived for between 2-7 years (depending on the contract) after project completion. All the project data will be moved into a secure file on our archives records (only senior management will have access). These folders will be deleted on reaching disposal trigger times.

Elemental:

If a project is complete, Elemental can suspend the project hub in question - effectively archiving that data from current referrals. When patient/project data has reached it's retention deadline, Elemental are contacted to remotely wipe the records.

Section 6: Information Handling Procedures

Information Handling Procedures ensure that personal information is protected and that it is not disclosed inappropriately, either by accident or design, whilst in use or when it is being transferred.

In line with legislation, personal information is not processed without a lawful basis being identified. **The Record of Processing Activities (ROPA) records all processing of personal data and identifies the legal basis for it being processed.**

These procedures cover all records which contain data or information which can be said to contain personal data whether stored in hardcopy or digitally.

Guidelines for staff on the secure use of personal information are outlined in the staff handbook, staff code of confidentiality and our **Data Security and Protection Policy.**

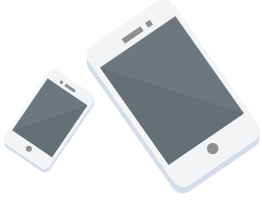
We ensure that there are secure points for the receipt of personal information transferred to us and we have applied the following measures to safeguard personal information during receipt and transfer/transit:

Verbal communications:

- Staff members have been provided with training on verbal communications. They know that they must take appropriate precautions not to reveal confidential information e.g. to avoid being overheard when making a phone call or not to have confidential conversations in public places or open offices. The staff handbook and their training inform them that breach of this procedure may be a disciplinary or legal offense.

Postal services and couriers:

We will ensure that all confidential information we transfer by post or courier is done so as securely as is practicable. All records transferred in this manner are addressed to a named individual and marked “Private and Confidential”. All records which are posted will be done through signed-for delivery so that it is guaranteed that the correct person receives the record.



Portable devices:

We recognise that information held on portable devices is at increased risk. Portable devices include memory sticks, CDs, DVDs, mobile phones etc. All portable devices have been documented on the **IAR,** and all relevant staff have received guidelines on safe usage and have signed a Portable Device Assignment Form. Due to the increased risk of viruses and the risk of losing data, the following procedures are followed:

- Laptops must be password protected with 2 Factor Authentication (both a password and pin code - compulsory for all laptops with access to Google Work Space).
- Password protected screensavers are installed on laptops,
- Anti-virus software is in use and is regularly updated.
- All portable devices are protected by either a PIN or password and/or fingerprint (dependent on the type of device).

Email:

We undertake that person identifiable information (either of employees or service users) can only be sent by secure email. Both the recipient and sender must have access to secure email.

Patient or service user information must only be sent via **nhs.net** emails or **Egress** email systems.

Section 7: GDPR subject access requests and rights

GDPR provides all individuals within the EU specific rights when it comes to their personal data.

To exercise these rights an individual should contact any staff member, though ideally the team manger and directors, and make a request either verbally or in writing.

In the instance that the request is made to a member of staff who is not the Team manager, that staff member will inform their Team manager and directors **as soon as possible**, the timeline for responding to requests begins from when the first staff member is contacted.

In all cases we will respond to a request without delay and in a timeframe not exceeding one month from when the request was made.

Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why it is required within one month.

- If the request is manifestly unfounded or excessive we may either request a reasonable fee to cover our administrative costs or we may refuse to comply with the request.

- If we refuse to comply with a request we will inform the individual why we are not taking action, tell them about their right to complain to the ICO, and tell them that they have the right to seek a judicial remedy.

- **In order to process any request, we will use reasonable means to verify the identity of the individual making the request so that no data is shared inappropriately.**

- The directors will maintain a log of all requests and their outcomes.

- **All staff will be informed of these procedures in our Data protection infographic.**

Subject Access Request Procedures

All individuals have the right to access their personal data which we process and store.

Confidential records of the deceased have the rights afforded to them by the Duty of Confidentiality and the Access to Health Records Act 1990. Should any person wish to request access for any records of the deceased they should contact the directors.

We will provide a copy of any information which it is lawful to provide free of charge. If further copies are required, we will charge a fee which will exclusively cover the administration costs of making copies.

We will provide copies of the information requested in a reasonable format – either in hard copy or digital.

Right to Erasure Procedures

All citizens have the right to request the erasure of their data which we control or process.

Citizens can request for their data to be erased in the following instances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When they withdraw consent;
- When they object to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed;
- The personal data must be erased in order to comply with a legal obligation;

We will not be able to honour any requests to have personal data erased when the data is being processed for the following reasons:

- to assess the working capacity of an employee;
- to provide a medical diagnosis;
- to provide health or social care or treatment or the management of health or social care systems and services;
- to exercise the right of freedom of expression and information;

- to comply with a legal obligation for the performance of a public interest task or exercise of official authority;

- for public health purposes in the public interest;

- archiving purposes in the public interest, scientific research historical research or statistical purposes;

- the exercise or defence of legal claims.

- Where at all possible, in the instance that we have appropriately shared an individual's records with any third-party we will inform this third-party of the erasure if appropriate.

- We will erase records in line with the disposal procedures set out above.

Right to Restrict Processing Procedures

All individuals have the **right to request that we restrict the processing of their data** in the following circumstances:

- while we are verifying the accuracy of any data we keep when an individual has made a request for the rectification of their personal data;

- in the instance that their personal data has been processed unlawfully and the individual requests that their data is not erased;

- When we do not need to keep the personal data but the individual has requested that we keep it in order to establish, exercise or defend a legal claim;

- If an individual objects to us processing their personal data, we will restrict all processing while we investigate the request.

When we restrict processing, we will store the individual's personal data but will not process their data in any other way.

If this is a **digital record** we can flag the patient data and code it to remove from reporting functions.

If the record is on **Elemental:** Elemental will be contacted to remove the individual's personal/identifiable details from the platform which means when running reports this info will not be included therefore we are restricting the processing of their personal data. However their pre and post scores which are not classified as personal/identifiable data will be included in the aggregate reports.

If this is a **paper record** - the individual's notes ad enrolment information will be moved this to the Data Processing Restrictions folder in the filing cabinet.

Right to Object Procedures

All people have the right to object to us processing their data in the certain circumstances.

They have an absolute right to object to us using their personal data for any direct marketing.

If they object to us using their data for marketing we will immediately stop using their data for this purpose. We will retain only enough data for us to be able to have a record that they don't want to receive direct marketing so that their request can be respected.

Individuals can also object to us processing their data if we are doing it under Public Task or Legitimate Interests grounds. The individual should provide specific reasons which are based on their specific situation for why they object.

We cannot comply with the objection if we have compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual or if the processing is for the establishment, exercise or defence of legal claims.

- In the instance that we cannot comply, we will clearly document our decision for this, inform the individual, inform them of their right to go to the ICO, or to seek judicial recourse.

Withdrawal of consent procedures

All people have the right to withdraw their consent to have their personal information shared at any time.

We guarantee that it will be as easy to withdraw consent as it is to give consent.

Paper Records:

The individual 's information will be changed to have a red sticker and a do not share with external partners/do not include in reports as appropriate to the request.

Digital Records:

On internal databases the individual 's information will be marked with a RED - do not share message/ do not include in reports as appropriate to the request.

For records on Elemental: The removal of clients will always be completed by Elemental at the request of Healthbox, Healthbox can only remove the client if there is no data attached.

If an individual withdraws their consent to share information we will discuss in full and explain how this decision may impact on their health and care outcomes.

In certain instances, where legislation or public good outweighs the individual's right to not consent to information sharing, we may not be able to honour any withdrawal of consent. This will be discussed in detail and will only occur if we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Any time in which consent is not given or is withdrawn the Team Manager and directors will keep a log of this and a note will be made on the individual's records.

Responsibilities

The directors are responsible for maintaining records around Subject Access, Rectification, Erasure and Withdrawal of Consent requests.

The Senior Management Team is also responsible for maintaining staff training on record keeping and auditing staff knowledge annually.

The Team Managers will report to Senior Management any Subject Access Requests or similar.

The directors will monitor compliance with the Data Quality & Record Keeping Policy and has responsibility for reviewing the policy at least annually.

Approval

This policy has been approved by the Senior Management Team and will be reviewed at least annually.

Last review date 29th June 2021

HEALTHBOX

COMMUNITY WELLBEING SERVICES