HEALTHBOX

COMMUNITY WELLBEING SERVICES

Data Security & Protection Policy

2021-2022

About this policy

This policy covers Healthbox CIC's responsibility to ensure data processing is performed in accordance with the General Data Protection Regulation 2018.
This policy outlines how GDPR relates to our organisation and what as staff you need to be aware of.

Who should read and understand this policy?

All Healthbox CIC staff including full and part time staff, sessional staff, volunteers and placement students or interns.

What is the purpose of the policy?

All Healthbox CIC staff need to be aware of, and adhere to our data security and protection policies and procedures. In order to safely and responsibly carry out our business contracts and services, client and participant data will be collected and stored and in some cases shared with relevant partners. This all comes under the term: **Data Processing.** As a business it is our responsibility to comply with all aspects of the 2018 GDPR. We recognise data protection as a fundamental right and embrace the principles of data protection by design and default.

This document also explains:

- Healthbox CIC's responsibilities
- Staff responsibilities
- What the GDPR involves
- How GDPR relates to the data we collect and our organisation
- Staff data leads
- Other policies and procedures you need to be aware of

Policy Statement

In order to ensure completion of business contracts and thereby maintaining and promoting excellence in working practice, client information will be collated and stored. In order for this to be achieved, clients will be aware of our Data Protection Policy at the start of the contract. It is our responsibility to adhere to the Data Protection Act of 1998 and GDPR (2018).

To achieve this Healthbox CIC will follow the below procedures:

1. Consent to collect client data shall be lawfully and informatively collected at the start of each new client contract/project enrolment.

2. Clients/participants will be asked for their consent for Healthbox CIC to use their information/name in any future marketing, promotional material or evaluation (where relevant). This consent will be in written form.

3. The data collected from the client/individual **will only be** information that services the needs of the contract for the duration of the contract.

4. We recognise that research documents such as published statistics are within the public domain and are therefore not required to be held in a secure manner.

5. Completed project/contract data will be kept as archive material. Therefore all data will be accurate to the time that the contract was live. We seek to obtain accurate and clear data for the duration of the live contract.

6. All documents/research that contain client data that was required for contract work by that client will be open for the client to inspect at their request.

7. Client data will be held securely in electronic format or where paper format is required within a locked cabinet within the locked premises of Healthbox CIC.

8. This client data will only be accessed by those members of staff that are working on the contract / project at the appropriate time.

9. At all times and in all places the named personnel will retain the confidentiality of those records.

10. Client data will not be forwarded to potential clients unless specific permission has been formally given in writing.

11. All Client data will remain within the United Kingdom.

Section 1: GDPR & Data Collection

GDPR & Individuals Rights

As part of our compliance with GDPR 2018 we ensure our procedures account for the rights of the individuals we work with:

- ✓ **The right to be informed**
- ✓ **The right of access**
- ✓ **The right to rectification**
- ✓ **The right to erasure**
- ✓ **The right to restrict processing**
- ✓ **The right to data portability**
- ✓ **The right to object**
- ✓ **The right to not be subject to automated decision making, including profiling**

Principles

We will be **open and transparent with service users** and those who lawfully act on their behalf in relation to their data processed and care and services they receive from us. We will adhere to our duty and responsibilities as a CIC and health providing service.

We will establish and **maintain policies to ensure compliance** with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

We will establish and maintain policies for the **controlled and appropriate sharing of service user and staff information** with other agencies, taking account all relevant legislation and citizen consent.

Where consent is required for the processing of personal data we will **ensure that informed and explicit consent will be obtained** and documented in clear, accessible language and in an appropriate format.

The individual can **withdraw consent at any time** through processes which have been explained to them. We ensure that it is as easy to withdraw as to give consent.

To adhere with the above rights Healthbox CIC ensures that procedures are in place to locate and delete a client's data easily and efficiently.

We acknowledge our accountability in ensuring that personal data shall be:

- ✓ **Processed lawfully, fairly and in a transparent manner**
- ✓ **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**
- ✓ **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')**
- ✓ **Accurate and kept up to date**
- ✓ **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')**
- ✓ **Processed in a manner that ensures appropriate security of the personal data**

Staff procedures and subject access requests

A Data Subject Access Request is a request from any data subject (client, service user, employee) to view the data held about them. They can ask for it to be modified, restricted or erased in line with the 8 GDPR rights.

- All staff handling personal data are required to complete in house training on the GDPR principles. Project managers will complete certified online training.
- If any staff member receives a subject access request, that staff member should report the request to the project manager/Healthbox CIC Director.
- The relevant staff member will verify the identity of the individual to protect against any potential data breach by asking questions based on the information held by Healthbox CIC.
- The Project Manager will be required to send the Healthbox CIC standard template letter and copies of any information held about that individual within 30 days of receipt and satisfactory verification of the individual's identity.
- In the event that the individual's identity cannot be satisfactorily verified, the subject access request will be denied and the individual referred to the ICO.
- Healthbox CIC reserve the right to refuse a request if unfounded or excessive. Healthbox CIC would inform the individual of this decision within a week of receipt of the request and explain the individual's right to complain to the supervisory authority and to a judicial remedy.
- Unless otherwise stated by the individual, any requested information will only be provided to that individual in the format in which it is held in by Healthbox CIC (electronic).
- Healthbox CIC will not charge/accept any financial payment for Subject Access Request process.

Documentation and Lawful processing of personal data:

Healthbox CIC lawfully processes personal data and will retain written consent by the individual or client organisation to hold that data.

Healthbox CIC recognises that the individual or client organisation has the right to **withdraw consent** to Healthbox CIC holding personal data at any point and request that this data is **deleted.**

Healthbox CIC will endeavour to explain data collection and usage procedures (for each individual project) to clients/participants as well as documenting these procedures securely in house.

We require the full and active participation of all our employees and volunteers in order that the principles outlined in this policy statement may be achieved.

Consent

In line with the GDPR standard of consent:

> *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"* GDPR definition

Healthbox CIC will ensure that lawful written consent is obtained before collecting, holding or processing any identifiable data about that individual/client. For virtual support, staff must explain why data is being collected and gain verbal consent.

Staff will be required to use the updated project enrolment form or complete the consent statement on Elemental to fully comply with this standard.

Children & Vulnerable Adults

Where consent is required for collecting, holding or processing any data for children or vulnerable adults, consent will be obtained from the relevant parent, guardian or legal advocate for that individual.

Data Breaches

Healthbox CIC recognises its responsibilities to put in place procedures to monitor and where necessary report data breaches to the ICO (Information Commissioner's Office).

Staff will be responsible for recording any **potential breach or near miss** and **reporting this to their project manager** or a Director immediately. Failure to comply will result in staff disciplinary measures. It will be at the discretion of the project manager/Director as to whether the breach could result in:

> *"Discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage."* GDPR 2018

If it is deemed that the breach could result in any of these outcomes, the breach will be reported to **both the ICO as well as those individuals directly involved.**

In response to a reportable data breach Healthbox CIC will conduct an **incident review** meeting with all involved staff members. The outcomes of this in terms of changes to policy and procedures effecting all staff will be shared as a **full team meeting**. This is in addition to Healthbox CIC complying to any conditions/guidelines provided by the ICO as a result of the breach.

What is Personal Data?

As defined by the GDPR, Personal Data is:

> Personal data means data which relate to a living individual who can be identified
>
> a. from those data, or
> b. from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
>
> And includes any expression of interest of opinion about the individual and any indication of the intentions of the data controller or any person in respect of the individual.
>
> GDPR 2018

Personal Data includes:

- Names
- Addresses
- Contact details such as phone numbers and email address
- Date of Birth
- Credit Card or account information

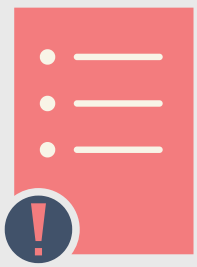
What is Sensitive/Special Categories of Data?

Sensitive personal data means data consisting of information as to:

a. the racial or ethnic origin of the data subject
b. the data subject's political opinions
c. the data subject's religious beliefs or other beliefs of a similar nature
d. whether they are a member of a trade union
e. their physical or mental health or condition
f. their sexual life
g. the commission or alleged commission by the data subject of any offence
h. any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings

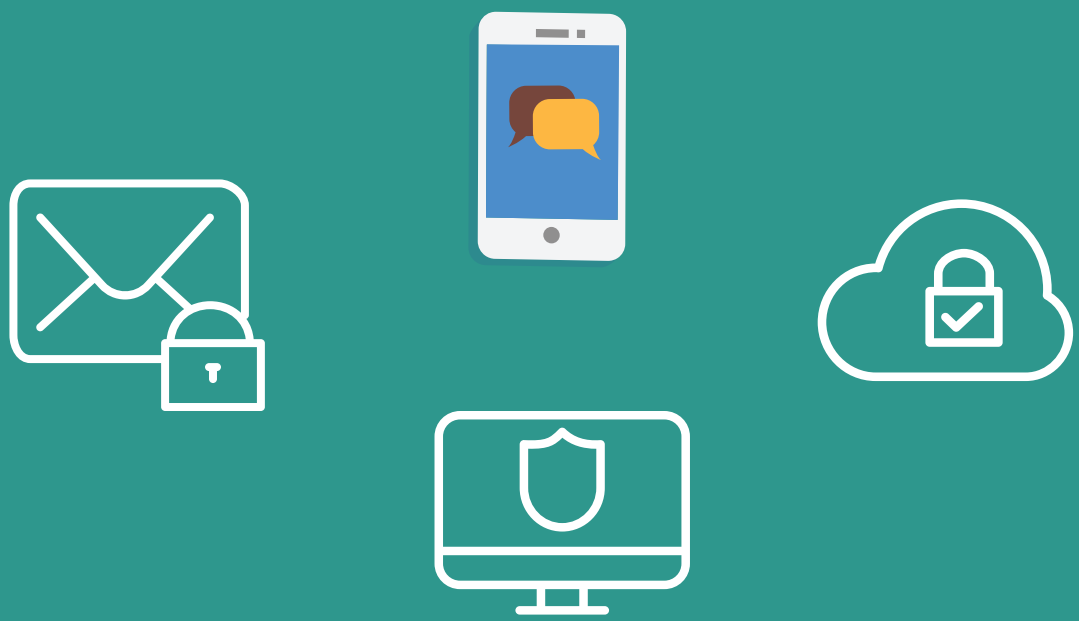
GDPR 2018

Collecting sensitive/special category data:



For our organisation the most common special category data collected is health information . This is to enable us to run safe, best practice activities and services.
At all times managers and staff must be aware of the data we collect and why we collect it - senior management will regularly review services and the data they collect to ensure only necessary data is routinely collected.

Section 2: Keeping data secure and Data Protection by Design



Safe storage, collection, sharing and transportation of personal data:

Much of the data collected from our participants and services users is in electronic format. If staff are speaking to a client on the phone they should complete any necessary paperwork/information digitally rather than writing paper notes where possible.

Data sharing between teams and partners is quite often necessary to deliver our services safely and effectively. Hubs and platforms such as Elemental, help this process. If you need to share data please consider the following and check the procedure with your line manager:

- Can the shared data have the PII removed? For example can codes be used instead of names?
- Almost all of our commissioned services only ever require **anonymised reporting** (for example number of service users accessing the services and average wellbeing scores). If you are being asked for PII to be included **ask why** and check with your manager before sharing data.
- How is the data being shared? Any data sharing containing PII must be through secure means such as NHS.net or Egress emails, or Elemental.
- Occasionally it may be necessary for a team to use password protected databases (this may be referrals for services/volunteer database etc). If you have a service database keep PII to the Absolute MINIMUM and never store this on your local drive on your laptop or a memory stick.
- When sharing details for referrals to external agencies, ENSURE you have CONSENT from the individual involved.

Healthbox CIC recognise that to safely conduct some of our services staff are required to carry some personal identifiable information with them when in a community setting. **To comply with GDPR principles when off-site all staff must:**

- Carry personal identifiable information in a **locked secure case**
- Keep the information **with them at all times** and not in public view
- Where possible this information should be in **electronic format** and on a duel authentication password protected device (see our password policy).
- **Never leave data unattended in a car/overnight**
- Data should be returned to Healthbox CIC office at the end of the day to be **locked away** and keys returned to the combination key lock box
- Personal data **must not** be transferred to USB/Memory stick/similar unless encrypted and signed off by a Healthbox Director
- Electronic personal identifiable information will be stored in secure area on Google Workspace or Elemental and **all devices must be locked (pin/password).**

Disposing of confidential data:

All paper **confidential waste** is stored securely and disposed of off-site using an accredited shredding service.

In the event of disposing of any portable electronic device that has been used to hold personal information, Healthbox CIC will ensure that the device hard drive is completely erased.

Reviewing policies and procedures:

As part of our commitment to data protection and security, each service and team will undergo internal annual reviews (or more frequently if required) which include assessments of data collection, storage and security protocols.

We will ensure we have sufficient resources and systems in place to support the policy requirements.

Our policies will be reviewed on an annual basis.

Data Protection by Design and Data Protection Impact Assessment:

As part of our GDPR compliance Healthbox has a an obligation to to implement both technical and organisational measures to integrate **data protection into all of our activities.**

This starts when we plan a project and continues throughout the delivery of the service to the end point including how long service data is stored after that project has finished.

To achieve this we will ensure:

- All new systems used for data processing will have data protection built in from the beginning of the system change.
- All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.
- We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

- In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

- Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

Privacy Impact Assessment

Healthbox CIC will conduct a **Privacy Impact Assessment** (PIA) for all new projects that include multiple partners and referral pathways.

Under the GDPR principles the following factors are likely to be included:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of an organisation.

PIA will be conducted by project managers with sign off where required by a director.

Process:

The PIA process is flexible and can be integrated into existing project management. The PIA should begin at the start/planning of a project, but can run alongside the project development process.

A PIA should include the following steps:

- Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes in the project plan
- Consult with internal and external stakeholders as needed throughout the process

ICO PIA Code of Practice

A checklist for screening the suitability of a PIA for projects is included in the Data Protection Policy File on shared drive.

If the data processing within a project is considered to be high risk for individuals following a PIA, then an additional **Data Protection Impact Assessment** (DPIA) will be conducted.

In this situation where Healthbox CIC believe they cannot sufficiently address the identified risks Healthbox CIC will consult with the ICO regarding the feasibility of continuing/initiating the project and maintaining full compliance with GDPR.

The following page is a template to enable staff to work through any new project, identifying the different stages of the data lifecycle and the questions they need to ask.

These questions can then be used to carry out a PIA including privacy risks and solutions with a senior member of staff.

New projects, PIA and identifying data flow stages

Security of data collection

What data is being collected?
Why is it being collected?
What is the benefit of the data collection?
What is the nature of the data collected? - only PII (personal Identifying Information) needs a PIA
What is the scope or volume of data being collected?

Security during processing

Where is the data being stored?
What format is the data in (electronic, paper)?
How is the data being used during processing?
Who has access to the data?
Are there any risks? (to the individual, to Healthbox or partners?)

Security during Sharing

Is the data being shared with partners?
Is there a data sharing agreement in place?
What are the legal reasons for sharing the data?
Does the data sharing require explicit consent? (Healthbox CIC informs all service users of any sharing of data with partners/third parties and consent must be gained)

Security during Storage/ archived project data

Where is the data stored/archived?
How long will it be stored or archived for?
Can the data be easily accessed for DSAR?
Who has access to archived data?
Are there any risks to this data?

Timing and methods of data deletion

When will archived data get deleted/destroyed?
How will this be done?
External platforms - data deletion request
Paper/wet signature documents (secure external shredding company)

ICO Registration:

All data is kept in accordance to the guidelines set out by the Information Commissioners Office ICO.

Registration Number Z3247753

Registration Start Date: 5th November 2012

Registration end date: 4th November 2021

Staff Training

As a member of the Healthbox CIC team, staff will complete data protection training.

This includes a Healthbox training video (general staff).

Team leads or those handling sensitive data will complete external training.

SIROs & data leads

Within the senior management team we have 1 SIRO and 2 Deputy SIRO's (Senior Information Risk Owners).

SIROs are responsible for embedding a culture of data protection within the organisation.

SIRO - Georgie Stanley (Director)

Deputy SIRO - Laura Turner (Director)

Deputy SIRO - Lorna Pearson (Finance)

Useful resources

ICO website:

www.ico.org.uk

Data Protection Act 2018:

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Other relevant Policies & Documents

Healthbox CIC Password Protection Policy

Data Breach and Near Miss flow chart and reporting procedure

Data Protection Staff Compliance Check List

PIA project template

Staff GDPR infographic

Service User GDPR infographic

Healthbox CIC Privacy Notice

Project Management & Data Reviews

Remote Working Policy

HEALTHBOX

COMMUNITY WELLBEING SERVICES