BSARCS GDPR & Data Protection Policy

ICO Registration Number: Z344654X (registered November 2012)

Introduction

The confidentiality, empowerment, consent and security of our clients (and their 'data') are core principles of BSARCS. BSARCS employees (and volunteers) are bound by these principles and must only store, access, process and share information about clients as is necessary to carry out their role. Employees and volunteers failing to comply with the policy may be subject to disciplinary procedures. Data protection is the fair and proper use of information about people and is part of the fundamental right to privacy. Our obligations as an organisation when dealing with personal information and data is set out in the Data Protection Act 2018 which sits alongside the General Data Protection Regulations (GDPR), both of which came into effect in the UK on 25 May 2018.

This document sets out our policies and procedures for BSARCS in line with DPA 2018 and the GDPR regulations.

This policy relates to BSARCS' therapeutic work only, records relating to our ISVA services are considered separately in the South Yorkshire Sexual Violence Partnership GDPR policy.

The Data Protection and GDPR Principles

Data Protection applies to the processing of personal information or data of any identifiable living person. Almost everything that we do with this information is regarded as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting of it.

The GDPR sets out seven key principles which are central to the protection of personal information. These principles and how we will comply with them is set out below:

- The principle of ***'lawfulness, fairness and transparency'*** – there must be valid grounds for collecting and using personal data and it must only be used in a way which is fair to the individual. Additionally, an organisation must be clear, open and honest with people from the outset about how their personal data will be used in order that they can make a decision about whether they wish to enter into a relationship with the organisation. *Consent will always be sought before a client's personal information is recorded with BSARCS, whether this is from the individual directly or confirmed to have been sought from the client by a referring agency. However, we also have a 'legitimate interest' for storing certain information about our clients and the service we have provided to them (for example, where a client may pose a risk to staff, where a service has been withdrawn or where we have exhausted our offer to an individual)*
- The principle of **'purpose limitation'** - the organisation must be clear from the outset on what data it intends to collect and for what purpose. It must also clearly *state* its purpose in order to be accountable and to ensure that individuals are able to understand how their data is to be used, are able to make decisions about what data they wish to share and assert their rights relating to their data. *BSARCS offers services to both adults and to children. The processes and purposes of data collection will differ dependant on the age group of our clients, and are set out in the appendices to this policy.*

- The principle of **'data minimisation' -** the data collected by the organisation must be sufficient for it to carry out its intended purpose but must be limited to that which is necessary and should not include irrelevant details. Any individual has the right to request that the organisation rectify inaccurate data or delete any data which is not necessary for the purpose of the organisation. *BSARCS has guidance relating to record keeping which should be read alongside this document. The process by which a client is able to exercise their right to erasure is detailed further in this documentation*;
- The principle of '**accuracy**' – an organisation must take all reasonable steps to ensure that any personal data held is accurate and an individual has the right to request that information be rectified where it is not. *BSARCS will respond to any request by an individual for us to rectify information held about them which is incorrect and, where appropriate, make the necessary changes. Any opinion recorded in a client's records will be clearly marked as such, this is detailed in the guidance on record keeping.*
- The principle of **'storage limitation'** – an organisation must not hold data for longer than is necessary for its intended purpose. *Having regard to the relevant statute, regulations and guidance BSARCS will generally retain client's personal information for 10 years from the date of their last contact or in the case of a child when they reach their 25th birthday if this is later (we also have specific retention periods relating to looked after children detailed in the Processing Documentation appendices) unless a client exercises their 'right to be forgotten' (see below) and we decide there to be no justification for retaining their personal information. In order to comply with our own retention periods, BSARCS will regularly (each quarter as a minimum)*
- The principle of **'integrity and confidentiality' (security)** - an organisation must process data in a manner which ensures appropriate security of the personal data, using technical and organisational measures to prevent unauthorised access, accidental loss, destruction or damage. *These measures are set out below.*
- In addition, the organisation shall be responsible for, and be able to demonstrate compliance with the principles set out above (**the principle of 'accountability'**)

Security of client information

BSARCS employees, volunteers, partners and other parties working on behalf of BSARCS must comply with the following measures for protecting client's personal data:

- Personal data must only be transmitted over secure networks
- All passwords used to protect personal data should not be shared, should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised. Passwords should not be saved in the browser if others have access to a shared computer, nor should they be written down where they may be easily accessed by others.
- Personal information contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely in the client's case management record. The emails should be deleted at the first opportunity
- All hardcopies of personal information should be stored securely in a locked drawer or cabinet.
- Employees must ensure that information which may identify a client is not left on their desk, on the photocopier or elsewhere at the end of their working day.

- Any loss of client information must be reported immediately to the Service Manager/ Data Protection Manager as this may constitute a breach of the GDPR regulations requiring a report to the Information Commissioners Office.

Taking personal information out of the workplace

Where possible employees should refrain from taking a client's personal information away from their place of work, this includes information stored on a laptop or tablet. However, if this is unavoidable or impractical then this information must be kept securely, must not be left unattended (i.e. in a vehicle) and should be returned to the office as soon as is practicable.
When it is necessary to take information away from the office, the information taken should be the minimum required to undertake the work and should not include identifying information.

Organisational measures to protect personal information

BSARCS takes the security of personal information seriously and has put in place the following measures in respect of the collection, holding and processing of personal data:

- BSARCS uses servers which are based in the AWS infrastructure and which make full use of the data security, availability and integrity features of this service
- Automated information back-ups are scheduled to run daily and are kept for a period of 7 days before disposal
- Search engine indexing is blocked to ensure that our system will not be found in search engines
- All data that we transmit to and receive from the server is encrypted
- Only authorised users are given access to client data, information is secured by a unique password. Accounts are disabled following repeated unsuccessful log-in attempts
- Staff accounts and access will be disabled promptly following an individual leaving the organisation
- Data access and modification is available only to authorised users
- BSARCS has a designated officer (data protection officer) with specific responsibility of overseeing data protection and ensuring compliance with the GDPR Regulations – this is currently Kirstin Evans, Business Manager
- All employees, volunteers, trustees, agents, consultants, partners or other parties working on behalf of BSARCS will be made fully aware of both their individual responsibilities and the organisation's responsibilities in regard to the protection of personal data and provided with appropriate training
- All employees and volunteers handling personal data will be properly supervised and supported in the processing of personal data
- The methods of collecting, storing and processing of personal data will be regularly evaluated and reviewed.

Individual's rights in relation to their personal information

The GDPR provides, amongst other rights, the following rights to an individual:

- The right to be informed

- The right of access
- The right to erasure

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data, this is a key requirement under the GDPR.
An organisation must provide individuals with information including, the purposes for processing their personal data, retention periods for their personal data, and who it will be shared with (this is called 'privacy information').
An organisation must provide privacy information to individuals at the time their information is collected; if information is provided by other sources (such as a referral from a professional), the organisation must provide individuals with this privacy information within a reasonable period and no later than a month.

BSARCS will issue privacy information (a privacy statement or notice) to all new clients which confirms how we will use their data and their rights relating to their data.

The right of access (subject access request)

Individuals have the right to access their personal data, this is commonly referred to as subject access. An individual may make a *subject access request* verbally or in writing.

The rights of access apply equally to adults and children. A child can make a subject access request where they are competent to do so. A parent or guardian can only exercise these rights on behalf of a child if the child authorises them to do so, when the child does not have sufficient understanding to exercise the rights him or herself, or when it is evident that this is in the best interests of a child. Records will only be released to a parent/ guardian where we are confident that this does not put the child at risk. Additionally, there are some GDPR exemptions relating to parental/ guardian access to child abuse data. As the requirements to respond to a subject access request from a parent/ guardian of a child or young person are extremely complex, any such request will be given careful consideration by the organisation.

It is also possible for a third party to make a subject access request on behalf of an individual but they must provide written evidence of their authority to act on the individual's behalf.
BSARCS will liaise directly with our client to confirm their authority and to discuss any implications of the information being provided; in all cases records will be provided to a client in the first instance, requiring written confirmation that the records may be provided to a third party before the request will be actioned.

A subject access request may be made directly to any employee within BSARCS, but upon its receipt this request should be passed to the data protection officer, who will log and acknowledge the request in writing. BSARCS will respond in full to the subject access request within 30 days of the request having been made.

BSARCS will not charge a fee for providing this information unless it is deemed 'manifestly unfounded or excessive' where we may charge a reasonable fee for the administrative costs of complying with

the request (this fee will be dependent on how much work is involved and how many copies are requested, but will not normally exceed £25).

The right to erasure

The GDPR introduces the right for an individual to have their personal data removed, this is often called 'the right to be forgotten', and is essentially an individual withdrawing their consent for our organisation to process their data.

Individuals are able to make a request for their personal data to be deleted verbally or in writing (which includes email). This request may be made to any employee within BSARCS, but upon its receipt this request should be passed to the data protection officer, who will log and acknowledge the request in writing.

BSARCS will respond to such requests within a month of it having been received, taking into account the regulations which apply, and giving particular consideration to request for erasure from children.

In considering a client's request for erasure, we will consider whether the interests of the organisation exceed that of the client and may make a decision to refuse the request, either fully or in part (i.e. we may decide it appropriate and just to retain information pertinent to the delivery of any future services). We may also retain anonymised data, such as demographics for the purpose of reporting to our funders.

A record must be retained of the removal of consent for six years after the deletion of records.

Associated Documents

- Client Privacy Notices
- BSARCS' Safeguarding Policies
- BSARCS' Confidentiality Policy
- BSARCS' Record keeping guidance
- BSARCS' ICT Policy
- SYSVP GDPR Policy
- BSARCS' Process for Provision of Case Notes

Appendix 1 – Processing Documentation

All information is recorded, processed and retained on the basis of consent. However, there may also be a legitimate business interest for retaining certain identifying data and this will be considered in the case of any request for access and erasure (for example that which is pertinent to risk and appropriate service delivery).

Adult clients

Clients are able to self-refer to the therapeutic services by telephone or webform, their personal information will be taken at the point of contact and added to our case management system in order that the referral can be actioned. The employee taking this information will explain to the individual the purpose of us taking this information.
Professionals are also able to refer clients by telephone or webform and will be asked to confirm that they have sought the consent of the individual to make the referral.

Information categories, storage and use

Item	Information	Stored	Purpose
1	Personal Information (name, address, DOB etc.)	BSARCS' CRMS database. Any paper forms capturing this detail to be shredded.	Contact Identification Safeguarding reporting
2	Demographics (gender, ethnicity etc.) & Vulnerability Data	BSARCS CRMS database. Any paper forms capturing this detail to be shredded.	Monitoring for funders and research (provided as quantitative data)
3	Specific categorisation of incidents under Sexual Offences Act 2003	BSARCS CRMS database. Any paper forms capturing this detail to be shredded.	Monitoring for funders and research (provided as quantitative data)
4	GP & Emergency contact	BSARCS CRMS database. Any paper forms capturing this detail to be shredded.	Emergency contact Safeguarding reporting
5	Interactions with Service	Stored on BSARCS CRMS database	Key information to manage referral/ casework appropriately and efficiently
6	Outcomes of support and service feedback	Stored in BSARCS CRMS database or on excel spreadsheet	Monitoring/ evaluation for funders (anonymised)
7	Materials created in sessions (drawings etc.)	Hardcopy will be stored securely until discharged at which point they will be offered to the client or destroyed.	Therapeutic

Sharing Information

We will not, without consent, share any information about a client unless we are compelled to do so by legal process (summons), there is an overriding safeguarding issue or it is deemed to be in the best interests of the client (see Safeguarding and Confidentiality policies). In these circumstances we will take all reasonable steps to inform the client of the request made and the information to be shared.

We will use information relating to the demographics of our clients, categorisation of sexual offence and outcomes to create a broad picture for funders and stakeholders to educate and inform around the impact of sexual violence and to evidence the need for funding streams to allow the development and continuation of the work of BSARCS.

Retention of information relating to Adult clients

BSARCS does not hold data for longer than is necessary for its intended purpose and in accordance with safe practice and therapeutic guidelines all adult data will be stored for 10 years after the last client interaction with our service. However, any client is able to make a request for their personal information to be removed and we will follow the procedures set out in the GDPR & Data Protection Policies to respond to this request.

Children's Services

Clients can be referred into the organisation by professionals, parents/ guardians or by self-referral. All professionals making a referral for a child will be required to complete a referral form and seek the child/ young person's written authority to refer as well as, where possible, the consent of the parent or guardian of that child.

We will accept a referral from a referring agency, and process information without the signed consent of a parent/ guardian only where the child/ young person has been assessed as 'Gillick/ Fraser' competent.

Information categories, storage and use

Item	Information	Stored	Purpose
1	Personal Information (name, address, DOB etc.)	Uploaded onto BSARCS CRMS database. Any paper forms capturing this detail to be shredded.	Contact Identification Emergency contact Safeguarding reporting
2	Demographics (gender, ethnicity etc.) & Vulnerability Data	Uploaded onto BSARCS CRMS database. Any paper forms capturing this detail to be shredded.	Monitoring for funders and research (provided anonymously as quantitative data)
3	Specific categorisation of incidents under Sexual Offences Act 2003	Stored on BSARCS CRMS database.	Monitoring for funders and research (provided anonymously as quantitative data)
4	GP & Emergency contact	Uploaded onto BSARCS CRMS database. Any paper forms capturing this detail to be shredded.	Emergency contact Safeguarding reporting
5	Interactions with Service	Stored on BSARCS CRMS database	Key information to manage referral/ casework appropriately and efficiently
6	Outcomes of involvement and service feedback	Either stored on BSARCS CRMS database or on excel spreadsheet	Monitoring/ evaluation for funders (anonymised)
7	Materials created in sessions (drawings etc.)	Hardcopy will be stored securely until discharged at which point they will be offered to the client or destroyed.	Worker and client's use

Sharing Information

As our Children's Services work with a systemic approach, we will work closely with parents and guardians and other agencies involved in supporting our clients. We will be clear with individual clients from the outset as to which agencies we will be involving in our support and all information sharing will be proportionate and only shared where this is deemed to be in the best interest of the client and to allow their support to be holistic. Additionally, we may share information where we are legally compelled to do so by legal process (summons) or where there is an overriding safeguarding issue.

Retention of information relating to the Children's Service

BSARCS does not hold data for longer than is necessary for its intended purpose and in accordance with safe practice and therapeutic guidelines all adult data will be stored for 10 years after the last interaction with our service, or the child's 25th birthday, whichever is later.

For children looked after by the local authority, in children's homes or who are adopted, the records will be retained for 75 years after the last interaction with our service.

However, any client is able to make a request for their personal information to be removed and we will follow the procedures set out in the GDPR & Data Protection Policies to respond to this request.