Data Protection Policy

BRITISH ASSOCIATION FOR PERFORMING ARTS MEDICINE

CARING FOR PERFORMERS' HEALTH

Category	Policy
Summary	This policy provides details of the principles and procedures BAPAM follows to meet the requirements of the Data Protection Act 1998 for handling personal information, with focus on 3 key priorities relevant to BAPAM's work: - personal data is relevant, accurate and good quality - personal data is kept securely and in the right hands; - processes for collecting and using personal data are transparent and open. The Policy applies to all BAPAM personnel
Valid From	1 November 2016
Version	2.0
Date of next review	November 2019
Approval Date/ via	BAPAM Board & BAPAM Medical Committee, 18 October 2016
Distribution	BAPAM Trustees & clinicians e-mail & online forum Staff e-mail and meetings Public website
Related Policies	*Access to Medical Records* *Confidentiality Policy* *Clinical Governance policy (& Clinician Agreement)* *Data Transmission Policy* *Employee Handbook* *Guidance for Handling Confidential Information when Working Remotely* *Healthcare Records Policy* *Incidents Policy* *Patient & Service User Contract* *Research Policy*
References	Data Protection Act 1998 - www.legislation.gov.uk/ukpga/1998/29/contents
Author	Dr Deborah Charnock, Chief Executive

1. Background & Purpose

This policy outlines how BAPAM meets its legal obligations concerning the collection and security of personal data as required by the Data Protection Act 1998 ('the Act'), including the Schedules and updates in force at the time of ratification of this policy.

BAPAM also has a duty to comply with guidance issued by the Information Commissioner's Office, the Charity Commission, the Care Quality Commission and the Fundraising Regulator and any other relevant guidance relating to the collection and handling of personal data.

2. Scope

This policy applies to all personnel working for BAPAM, including Trustees, employees, clinicians, and volunteers .

It applies to all data which is 'about' an identifiable, living individual that is held in any format including, but not exclusively, written and electronic information.

Data Protection legislation consists primarily of guidance which organisations must consider when handling personal data. Compliance requires applying the eight Principles of the Act in ways that are appropriate to the organisation's context, balancing statutory guidance with the organisation's mission and ethos.

Within the context of BAPAM's work and mission, our data protection policy and practices focuses on 3 key priorities:

- collecting information that is **relevant, accurate** and **good quality**
- keeping information **securely** in the **right hands**
- **openness and transparency** about the use of personal data, taking account of the legitimate concerns of individuals about the ways in which their data may be used and to whom it may be disclosed

3. Definitions

Data Subject is the living individual to whom personal data relates.

Personal Data is defined under the Act as that which relates to a living individual who can be identified from that data or from any other information which is in the possession of, or likely to come into the possession of, the *Data Controller* (see below). It may include any expression of opinion about the individual and any intention of the data controller or any other person in respect of the individual.

At BAPAM, the types of personal data held relate to:

- personnel - employees, Trustees, clinicians and volunteers
- service users:
    - performers contacting BAPAM's Helpline
    - performers registered on BAPAM's database for access to Directory practitioner referrals and BAPAM clinic appointments
    - participants attending BAPAM education and training events
    - visitors to BAPAM's website
- subscribers and supporters:

- Healthcare practioners approved by BAPAM's Medical Committee for listing as members of the Directory of Practitioners
- Members of any BAPAM Friends, Subscriber and Supporter schemes

***Sensitive* Personal data** is personal data that has the potential to be used in ways that are discriminatory or harmful to the data subject if shared inappropriately, and as such, require higher standards of security than some other forms of personal data.

Sensitive personal data is information about a data subject's: racial or ethnic origin; physical or mental health or condition; sexual life; political opinions; religious or other beliefs of a similar nature; membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992); the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. BAPAM collects *sensitive personal data* about personnel and about performers registered on the database for access to BAPAM healthcare services (clinic appointments and referral to Directory practitioners).

A ***Data Controller*** is the person within an organisation who determines (either alone or jointly or in common with other persons) the purposes for which and the manner in which any personal data is processed. The Data Controller must exercise control and take responsibility for the data protection of the information belonging to that organisation. This includes any agreements and contracts with third parties accessing that data – i.e. *Data Processors* (see below). At BAPAM, the *Data Controller* is currently the Chief Executive.

A ***Data Processor*** is any person(s), other than an employee of the Data Controller, who processes the data (notably personal data) on behalf of the *Data Controller*. At BAPAM, *data processors* are most commonly independent contractors providing IT services (management of computers, database, website, mailing lists etc), as well as accountancy and human resources support. It may also include independent organisations and professionals working with BAPAM on shared patient care or research initiatives.

Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.

A ***Healthcare Record*** for the purposes of the Act is one which relates to the physical or mental health of an individual which has been made by or on behalf of a health professional in connection with the care of that individual.

4. Legal Framework

Although BAPAM is not a statutory service provider, it has a duty to comply with the Act and guidance issued by the Information Commissioner's Office (ICO) (and maintains an up to date notification with the ICO), the Charity Commission (Charities Act 2011) and the Care Quality Commission (Health & Social Care Act 2008) and to take into account relevant guidance issued by the Department of Health, the NHS Executive and the Fundraising Regulator relating to personal data management. BAPAM's policies and procedures for management of personal data also takes account of additional relevant legislation listed below:

- *Access to heath records 1990*
- *Access to medical reports act 1998*
- *Safeguarding Vulnerable Groups Act 2006*
- *Health & Social Care Act 2008*

- *Human Rights Act 1998*
- *Privacy & Electronic Communications Regulations (PERC) 2003*
- *Serious Crime Act 2015*

5. Responsibilities

The BAPAM Board of Trustees has overall legal responsibility for Data Protection compliance.

Day to day responsibility for Data Protection is delegated to the **Chief Executive** as the Data Controller. The main responsibilities are:

- Briefing the board on BAPAM's Data Protection responsibilities
- Developing, monitoring and reviewing Data Protection and related policies and procedures, including preparation of *Incident* reports and action plans involving Data Protection breaches and 'near misses' for the BAPAM Board and Medical Committee
- Advising staff and personnel on Data Protection issues
- Ensuring that Data Protection induction and regular training takes place
- Approving unusual or controversial disclosures of personal data (in consultation with the Medical Director or a nominated Trustee where appropriate)
- Approving contracts with Data Processors
- Maintaining up to date Notification with the Information Commissioner's Office
- Handling requests from individuals for access to their personal data (personnel and service users)

The **BAPAM Clinics Manger** has the following responsibilities:

- Assisting the Data Controller in identifying aspects of their area of work which have Data Protection implications so that guidance can be provided as necessary
- Ensuring that all BAPAM activities take full account of Data Protection requirements, and filing *Incident reports* and implementing action plans where required
- Including Data Protection and confidentiality in the induction and training of all staff and volunteers.

The **Honorary Medical Director** is responsible for supporting and advising the BAPAM Chief Executive, Clinics Manager and staff on specific Data Protection issues as they relate to BAPAM's *Clinical Governance policy* and healthcare management procedures.

All **BAPAM personnel** (Trustees, staff, clinicians and volunteers) are responsible for understanding and complying with this policy and the procedures that BAPAM has adopted in order to ensure Data Protection compliance.

6. The Eight Data Protection Principles

The Act imposes obligations on anyone who processes personal information to do so in accordance with the Eight Data Protection Principles and Schedules under the Act. These set down a framework for the lawful processing of data. A fundamental element of the Act is that it gives an individual the right to consent to their data being collected and used, to access the data held about them, and to have the data corrected or deleted where appropriate.

The Eight Principles and notes on BAPAM's general procedures for dealing with them are outlined in the section below. Additional, detailed operational considerations are outlined in Sections 7 – 9, and in the Appendix.

Principle 1: Personal data shall be processed fairly and lawfully, and in particular shall not be processed unless:

a. ***At least one of the conditions of Schedule 2 of The Act is met, and***
b. ***In the case of sensitive personal data, at least one of the conditions in Schedule 3 of The Act is also met.***

(Full details of the Schedules can be seen at www.legislation.gov.uk/ukpga/1998/29/contents)

In brief, to comply with Principle 1, BAPAM will always ensure that:

- there are legitimate grounds for collecting and using the personal data
- the data subject has given consent for their data to be processed
- the data is not used in ways that have unjustified adverse effects on the individuals concerned
- all the individuals about whom data is collected are made aware of the uses that BAPAM makes of information about them
- staff handle people's personal data only in ways it would be reasonable to expect.
- BAPAM does not do anything unlawful with the data

Additional considerations concerning the processing of **sensitive personal data** as outlined in Schedule 3 of the Act are:

BAPAM processes information about a person's ***physical and mental health*** (including ***sexual life*** where relevant) as necessary for ***medical*** purposes. Processing is only undertaken by:

- a health professional, or
- a person who, in the circumstances, owes a duty of confidentiality equivalent to that which would arise if they were a health professional

Medical purposes includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services

BAPAM processes information about a data subject's ***racial or ethnic*** origin as necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained in all BAPAM's services and operations

BAPAM processes information about ***membership of a trade union*** as follows:

i) performers registered on BAPAM's service user database: for anonymised service activity reports to Trades Union organisations who are BAPAM funders

ii) employees: in cases relating to employment legislation

Principle 2: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

BAPAM will always:

- be clear from the outset about why it is collecting personal data and what it intends to do with it
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data

- comply with what the Act says about notifying the Information Commissioner
- ensure that if BAPAM wishes to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

BAPAM ensures that:

- it holds personal data about an individual that is sufficient for the purpose we are holding it for in relation to that individual
- it does not hold more information than we need for that purpose.

Principle 4: Personal data shall be accurate and, where necessary, kept up to date.

BAPAM ensures that:

- it takes reasonable steps to ensure the accuracy of any personal data it obtains
- the source of any personal data is clear
- it carefully considers any challenges to the accuracy of information
- it considers whether it is necessary to update the information.

Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

To comply, BAPAM

- regularly reviews the length of time it keeps personal data
- considers the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it
- securely deletes information that is no longer needed for this purpose or these purposes
- updates, archives or securely deletes information if it goes out of date.

Specific operational details relating to BAPAM's personal records management in relation to Principles 3 to 5 are outlined in the *Access to Medical Records Policy, Healthcare Records Policy*, *Employee Handbook,* and *Clinician Agreement*. Retention/destruction schedules are also summarised in the attached Appendix.

As patient records – both electronic and hard copy – contain extensive *sensitive* personal information, BAPAM considers retention and destruction particularly important. Hard copies are destroyed after **ten years** except for patients under 18 – these records must be retained until 28 years of age (our insurer's requirement). A comprehensive programme for electronic record archiving and destruction is currently in development, and will be overseen by the Medical Committee.

Principle 6: Personal data shall be processed in accordance with the rights of data subjects under this Act

To comply, BAPAM has procedures in place which ensures data subjects have:

- a right of access to a copy of the information comprised in their personal data
- a right to object to processing that is likely to cause or is causing damage or distress

- a right to prevent processing for direct marketing
- a right to object to decisions being taken by automated means
- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- a right to claim compensation for damages caused by a breach of the Act.

Additional relevant policies include *Healthcare Records Policy, Access to Medical Records policy* and *Employee Handbook.*

Principle 7: Appropriate technical and organisational measures shall be taken against un-authorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In practice, Principle 7 requires BAPAM to have appropriate security to prevent the personal data we hold being accidentally or deliberately compromised. In particular, we:

- design and organise security to fit the nature of the personal data we hold and the harm that may result from a security breach
- are clear about who in BAPAM is responsible for ensuring information security
- make sure BAPAM has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff
- are ready to respond to any breach of security swiftly and effectively

Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This principle has implications for contracts with Data Processors, particularly IT providers processing and storing data on BAPAM's behalf - including any cloud-based products. The BAPAM Chief Executive is responsible for all contractual arrangements. Key guidelines are outlined in the Appendix.

7. BAPAM's Security Procedures:

BAPAM treats all personal data as confidential and keeps it secure and accessible only to authorized personnel. The following security measures are in place:

All personal data is permanently stored in BAPAM's administrative offices, which are always self-contained and accessible only to authorised BAPAM personnel. All electronic data is stored on the secure server located in the admin office. Patients' hard copy, confidential medical records are held within a locked inner office. All restricted personnel records are stored in locked filing cabinets, which are only accessible to the Chief Executive, Clinics Manager or nominated Trustee (see Employee Handbook).

In London, hard copy patient notes for clinics and clinician dictation tapes are transported in a labelled 'Confidential' notes bag, which is only accessible to authorised BAPAM staff. They are returned to secure storage in the office immediately after the end of a clinic day. Patient notes cannot be removed from the office for any purposes other than these clinic consultations.

BAPAM operates a clear desk policy: staff keep all information out of sight of unauthorised personnel by keeping desks clear of confidential information.

All staff PCs are password protected and screens time out after 3 minutes.

Similarly, all telephone conversations are kept confidential. Stored Helpline messages can only be accessed by authorised staff through the Admin office telephone, which is password protected.

All personal data in electronic format (CRM database, personnel files, patient letters/reports, accountancy files) is currently stored on a secure server located in the BAPAM administrative office and only accessible on networked office PCs by authorised BAPAM personnel. No personal data is currently available on the web with the exception being the contact details for Directory Practitioners, which are made publicly available on the BAPAM website with the explicit consent of the Practitioner.

A cloud-based data management system, including a full electronic patient record, is currently being considered. Contractual arrangements will ensure compliance with the Act as outlined in the Appendix.

BAPAM uses anonymised online survey forms to gather feedback from service users. No personal identifiable information (including IP addresses) is collected via these forms.

All data security arrangements are under constant review and are discussed annually either at the Board or Medical Committee.

BAPAM takes particularly seriously the storage and transmission of *sensitive* personal information in electronic format. Details are outlined in the *Data Transmission Protocol* (note that this requires that all e-mail communications containing sensitive personal information must be encrypted).

Procedures for processing personal information remotely (e.g. Regional Clinicians, staff working in clinic away from the Admin office) are outlined in the *Guidance for Handling Confidential Information When Working Remotely.* Again, a central requirement is that sensitive personal information should not be downloaded or stored on personal or mobile devices in an unencrypted format.

BAPAM monitors data security issues through Data Controller/Processor contracts and staff training. Any breaches, including 'near misses', are logged as Incidents (see *Incidents Policy*) and are discussed in detail at BAPAM staff and Medical Committee meetings, as well as in regular summary reports to the Board. Action plans arising from *Incident* report may include updates to policies and procedures.

8. Information and Consent

BAPAM informs personnel about the processing of their personal data through contractual information (see *Employee Handbook* and *Clinicians Agreement)*.

BAPAM informs registered service users about the processing of their personal data through the *Patient & Service Users Contract,* and through additional written and verbal communications with service users (registration and appointment e-mails and telephone calls). All staff are trained in providing this information.

Clinicians also record in patient's notes any discussions relating to personal data processing (e.g. sharing information for referrals) arising from the clinical consultation and in communications with authorised personnel involved in the patient's care (see *Healthcare Records Policy* and *Clinician Agreement*).

Although there is currently no specific legal requirement to gain consent for marketing, BAPAM's policy is to inform service users – i.e. performers registering with us and participants at BAPAM events - that their e-mail address will be added to an online mailing list for notifications of events and activities including fundraising initiatives. Procedures for opt-out are provided.

If a registered performer is offered an appointment at a BAPAM clinic, they are also informed in advance that they will be asked for a donation to support BAPAM's work.

All BAPAM direct marketing is conducted via e-mail: we do not undertake marketing via personal letters, SMS messages or telephone calls.

BAPAM never offers data subjects' contact details to third parties for independent marketing purposes.

Visitors to the BAPAM website are informed about the site's use of *Cookies* under the Legal or Privacy section of the website.

9. Sharing information

BAPAM's policy is that personal data should only be shared if explicit consent from the data subject has been given. Further details regarding the circumstances and process for sharing are outlined in the *Confidentiality* and *Data Transmission Policies.*

Occasionally, data relating to BAPAM personnel or patients may need to be shared without consent – for example, *Incidents* where there are criminal or *Safeguarding* concerns. In these circumstances, the BAPAM CEO and Clinics Manager will act in accordance with relevant BAPAM policies and national guidelines (including Schedules relating to the Data Protection Act, as well as the Serious Crime Act 2015 and Safeguarding Vulnerable Groups Act 2016) and in consultation with the Medical Director or a nominated Trustee where appropriate.

Note that personal data contained in routine *Incidents Reports* to BAPAM's Medical Committee is pseudonymised through use of their unique CRM database ID number: the identity of the patients and personnel described in these reports can only be decoded by authorised BAPAM staff, and some items may be excluded or circulation restricted to further protect a data subject's identity.

10. Training

BAPAM staff receive Data Protection training on induction, and all personnel receive regular notifications and updates from the Chief Executive and Clinics Manager about Data Protection issues.

11. Breach of policy

All BAPAM personnel will receive a copy of this policy and will be required to comply as a condition of working at BAPAM.

In certain instances, breaches of the policy may constitute professional misconduct and could lead to disciplinary action.

Version 1.0 = 30 Oct 2013 (D Charnock); Updated 28 Apr 2015 (D Charnock). Reviewed April 2016 (D Charnock, R Whiticar)

Version 2.0 = 1 November 2016 (D Charnock)
Next Review = November 2019

APPENDIX

1. Summary of personal data collected at BAPAM

Data Subject	Personal data	Sensitive data collected	Purpose for collecting personal data	Informed about Purpose; Consent issues	Format/location	Retention period
Employees	i. Identity & contact details ii. Qualifications & Educational history iii. Application, appraisal & Performance data iv. Next of kin contact details v. Finance & benefits data (payroll, pensions, statutory leave)	Health; ethnicity; DBS check notification Union details (non-routine)	Appropriate workforce for delivering BAPAM's mission/operations Safeguarding Legislation Employment Legislation	Issued with contract Sharing contact details: professional = consent implied; Personal (eg home email addresses) = consent required.	Name & contact details on CRM database All other information held in subject's individual electronic and paper records Finance held in accounting system DBS information processed by online Umbrella Organisation.	6 years Failed job applicants = 6 months DBS Check background information = 6 months
Trustees, Committee members, Assessing Clinicians,	i. – iii. above Some financial details for expenses claims	DBS check notification	Appropriate workforce for delivering BAPAM's mission/operations	As above	As above	As above

Volunteers			Charity Law (includes Safeguarding)			
Directory Practitioners	As above	DBS check notification	For 'approval' as fit and suitable practitioners to take referrals	Directory practitioners can opt to have their name, contact details and qualifications displayed publicly on BAPAM website: consent given in Application.		As above
Performers registering with BAPAM	Identity & Contact details; demographic details; performance training and practice;	Yes: Health; ethnicity; union membership	For benefitting from BAPAM network/information/ support including mailing list Monitoring & reporting (anonymised)	Information about purpose & consent for processing issued at time of registration (verbal and automated e-mail) Information & consent for mailing list issued at time of registration (automated e-mail) Offered opt-out of mailing list Consent for sharing contact details with third parties involved in care (i.e. referral to Directory Practitioner) - verbal agreement with Team member	CRM database	10 years (or until 28 if under 18)

Performers attending BAPAM clinical assessment	Healthcare record created in addition to above	Yes – as above at registration Patient ntoes - health status, medical history (symptoms, therapies, diagnosis), referral and care plan. Could include psychological Sexual, Safeguarding issues	As above *plus* direct provision of care	As above Also appointment confirmation e-mail link to Patient Contract Consent for sharing contact details with third parties (e.g. referral to funding organisation, referral to Directory Practitioner) - verbal agreement with Team member Consent for sharing details including healthcare record with other healthcare professionals – verbal agreement with Clinician; recorded in patient notes	Healthcare record – individual's electronic & paper record Survey monkey paper or online feedback form (anonymous)	10 years (or until 28 if under 18) Survey data (anonymous) = 6 years (online version only)
Education & training participants (open access events)	Name & contact details	No	Mailing list Monitoring & reporting (anonymised)	Purpose & mailing list - Issued with confirmation of event registration (automated email) Offered opt-out of	CRM database Some paper records Survey Monkey online feedback form (anonymised)	Mailing list = refresh every 2 years Survey data (anonymous) = 2 years

				mailing list Offered opt-out of sharing name and contact details with event participants		
Mailing list subscribers/ Friends/Supporters	Name & contact details Note: personal financial details are not collected or stored on BAPAM system	No – unless registered performers	Mailing list	Purpose, mailing list and possible web listing - Issued with confirmation of registration Offered opt-out of mailing list Offered opt-out of listing on Supporters page	CRM database Some paper records Survey monkey forms (anonymous)	Refresh every 2 years 'Unsubscribers' = immediate. Surveys (anonymous = 2 years)

2. Checklist for BAPAM when contracting Data Processing services:

1) Is it clear that you are the Data Controller and the external organisation is a Data Processor?
2) Have you specified (in general or specific terms) the data to be used and the purpose for which it is to be used?
3) Is it clear that all data supplied by you is confidential (unless it is legitimately in the public domain), and that the Data Processor must not misuse the data or disclose it without your consent or retain it after completing its work on your behalf?
4) Is it clear how you authorise the activities of the Data Processor (e.g. specifying which of your staff can issue instructions to the Data Processor)?
5) Does the contract require the Data Processor to have effective security (including technical measures, and measures to underwrite the probity of staff), and to permit you to audit this effectively? (You may want to annexe to the agreement a list of agreed security measures based on your own security policy.)
6) Have you set out a means of secure transmission of data between you and the Data Processor?

7) Is the Data Processor required to inform you immediately of any security breach they become aware of (whether they caused it or not)?
8) Does the Data Processor indemnify you for any costs incurred in putting right breaches of Data Protection brought about deliberately or negligently by the Data Processor (ideally including costs of reassuring affecting individuals, even if this is not legally required)?
9) Is the Data Processor required to promptly forward to you all subject access requests and complaints about any of the processing?
10) Is the Data Processor required not to process the data, or allow it to be processed, outside the European Economic Area without your prior consent?
11) Is the Data Processor required not to sub-contract any of the work without your prior consent?
12) Is the Data Processor required not to do anything which would put you in breach of the Data Protection Act.