Data Protection Policy

Category	Policy
Summary	This policy provides details of the principles and procedures BAPAM follows to meet the requirements of the Data Protection Act 1998 and GDPR 2018 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	October 2024
Version	3.2.1
Date of next review	October 2027
Approval Date/ via	BAPAM Board & BAPAM Medical Committee, October 2024
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 2018 https://www.gov.uk/government/collections/data-protection-act-2018 GDPR guidance, ICO
Author	Claire Cordeaux, CEO

Amendment Log			
Amendment date	**Version**	**Additions or Alterations**	**Initials**
Feb-2026	3.2.1	Interim update pending comprehensive review Clarification of BAPAM's regulatory status and obligations, including CQC and SEQOHS statuses.	FR

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 2018 ('the Act') and UK GDPR, 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, and the Fundraising Regulator, and any other relevant guidance relating to the collection and handling of personal data.

In relation to medical records, BAPAM must also comply with additional legislation including the common law duty of confidentiality, and any other relevant legislation and professional guidance governing the retention, security, and confidentiality of medical records.

2. Scope

This policy applies to all personnel working for and contracted by 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 seven 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 (natural persons) is the living individual to whom personal data relates.

Personal Data. Under the DPA 2018, personal data refers to any information relating to an identified or identifiable living individual – that is, an individual who can be identified directly or indirectly by the data. This includes names, identification numbers, location data, online identifiers or one or more factors specific to them, such as physical, physiological, genetic, mental, economic, or cultural information, or their social identity. Effectively, anything that could be used to identify an individual in some way is considered personal data, which includes more modern factors such as internet IP addresses

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

- personnel - employees, Trustees, clinicians and volunteers
- service users:
    - Performance professionals contacting BAPAM's Helpline
    - Performance professionals 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 practitioners approved by BAPAM's Medical Committee for listing as members of the Directory of Practitioners
    - Members of any BAPAM Friends, Subscriber and Supporter schemes

Special Categories of 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.

Special Categories of 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 ; the commission or alleged commission by the data subject 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 *personal data* about personnel and about performance professionals registered on the database for access to BAPAM healthcare services (clinic appointments and referral to Directory practitioners).

A ***Data Controller or 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 CEO.

A ***Data Processor or 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 UK GDPR and Data Protection Act 2018. BAPAM must also comply with the common law duty of confidentiality in relation to medical records and special category data, and take into account relevant guidance issued by 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 health 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*
- *Equality Act 2010*

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 **CEO** 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 breach (*Incident)* reports and action plans involving Data Protection breaches and 'near misses' for the BAPAM Board and Medical Committee
- Reporting relevant breaches to the ICO within 72 hours
- 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 Senior Manager, Special Projects** has the following responsibilities:

- Delegated authority from the CEO for responsibilities listed above as follows:
- Briefing the Data Controller in identifying aspects of their area of work which have Data Protection implications and advising on guidance if necessary
- Reviewing Data Protection and related policies and procedures, ensuring that all BAPAM activities take full account of Data Protection requirements, and filing *Incident reports* and advising on and implementing action plans where required
- Advising and training and inducting staff on data protection issues
- Monitoring contracts with Data Processors

The **Medical Director** is responsible for supporting and advising the BAPAM CEO, Senior Manager, Special Projects, 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 Seven Data Protection Principles

The Act imposes obligations on anyone who processes personal information to do so in accordance with the Seven 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 Seven 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 transparently

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 is asked for consent in a clear and unambiguous way and consent for their data to be processed has been recorded, including recording where consent has been subsequently withdrawn
- 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

There are additional considerations concerning the processing of **special categories personal data**. 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 used only for specified, explicit 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 and GDPR 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 limited to only what is necessary. (Data minimisation)

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 *Special categories* personal information, BAPAM considers retention and destruction particularly important. Hard copies are destroyed after **eight years** except for patients under 18 – these records must be retained until 26 years of age (our insurer's requirement).

Principle 6: Appropriate technical and organisational measures shall be taken to ensure the integrity and confidentiality of data and to guard against un-authorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In practice, Principle 6 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 7: BAPAM will be able to demonstrate accountability to UK GDPR and the Data Protection Act 2018.

This principle ensures that BAPAM is responsible for complying with the UK GDPR and can demonstrate compliance through appropriate technical and organisational measures to meet the requirements of accountability.

This includes

- adopting and implementing data protection policies;
- taking a 'data protection by design and default' approach;
- putting written contracts in place with organisations that process personal data on our behalf;
- maintaining documentation of our processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a data protection officer
- adhering to relevant codes of conduct and signing up to certification schemes.

Accountability obligations are ongoing, and measures must be regularly documented, reviewed, updated and reported to the Medical Committee and Board.

7. BAPAM's Security Procedures:

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

All hard copy personal data is permanently stored in BAPAM's administrative offices, which are always self-contained and accessible only to authorised BAPAM personnel, confidential medical records are held in a locked cupboard. All electronic data is stored on the secure Microsoft cloud server which is GDPR and HIPPA Compliant and stored on a server in Dublin with backup in Berlin. All restricted personnel records are stored in locked filing cabinets, which are only accessible to the CEO or nominated Trustee (see Employee Handbook).

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 and held in a confidential space using headphones. Stored Helpline messages can only be accessed by authorised staff through the administration telephone, which is password protected.

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

All data security arrangements are under constant review and are discussed as a standing item either at the Board or Medical Committee.

BAPAM takes particularly seriously the storage and transmission of *Special categories* personal information in electronic format. Details are outlined in the *Data Transmission Protocol* and personal medical information is encrypted.

Procedures for processing personal information remotely (e.g. Regional Clinicians, staff working remotely) 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.

Data storage is stored online in Dublin with backup in Berlin which meets with the EU adequacy decision, and we have checked that we are compliant with the ICO. Contracts with Data Processors all meet this requirement.

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*).

BAPAM's policy is to inform service users – i.e. performers registering with us and participants at BAPAM events – of our privacy policy BAPAM Legal Information | Performing Arts Medicine as well as our Patient Contract and Consent statement Patient-Contract-Consent-2018-v2.pdf (bapam.org.uk). We need agreement from patients to subscribe to our newsletter and 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.

Data Protection Impact Assessments (DPIA)

The GDPR includes an obligation to conduct a DPIA for types of processing likely to result in a high risk to individuals' interests. The Information Commission Office (ICO) guidance is that DPIAs are required for projects using data which:

- uses systematic and extensive profiling with significant effects;
- processes special category or criminal offence data on a large scale
- systematically monitors publicly accessible places on a large scale.

The ICO also requires a DPIA if there are plans to:

- use new technologies
- use profiling or special category data to decide on access to services
- profile individuals on a large scale
- process biometric data
- process genetic data
- match data or combine datasets from different sources
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')
- track individuals' location or behavior
- profile children or target marketing or online services at them
- process data that might endanger the individual's physical health or safety in the event of a security breach.

BAPAM will consider a DPIA for any major new data projects which involves the use of personal data, these are likely to include:

- updating the database (CRM)
- providing access to researchers
- introducing new technologies for smarter working (e.g. text messaging patient reminders)

Right of access

Personal data is 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, in electronic format if this is how the information is stored
- 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 to have inaccurate personal data corrected
- a right to have data erased, unless there is good reason not to do so
- a right to have their data transferred directly to another provider
- 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*.

Individuals have the right to access their personal data and supplementary information so that they are aware of and can verify the lawfulness of the processing. This includes:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – mainly the information that should be provided in privacy notice

BAPAM will provide a copy of the information free of charge unless the request is manifestly unfounded or excessive, particularly if it is repetitive in which case the CEO will decide whether a fee should be levied on the administrative cost of providing the information. The information will be provided within one month, although can be extended to a further two months where requests are complex or numerous. If this is the case, the individual will be informed within one month of the receipt of the request as to why the extension is necessary.

BAPAM will verify the identity of the person making the request, using 'reasonable means', and if the request is made electronically, the information will be provided in a commonly used electronic format.

BAPAM will work towards the GDPR best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information.

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 Medical Director 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 Director and Clinics Manager about Data Protection issues.

11. Breach of policy
It is a legal requirement to report a personal data breach to the ICO under the GDPR if it is likely to result in a risk to people's rights and freedoms. If there is the likelihood of a *high* risk to people's rights and freedoms, the breach also needs to be reported to the individuals who have been affected.

High risk situations area likely to include:

- the potential of people suffering significant detrimental effect – for example, discrimination, damage to reputation, financial loss, or any other significant economic or social disadvantage.

Under the GDPR there is a requirement for organisations to report a personal data breach that affects people's rights and freedoms, without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Organisations will have to provide certain details when reporting, but the GDPR says that where the organisation doesn't have all the details available, more can be provided later. The ICO will not expect to receive comprehensive reports at the outset of the discovery or detection of an incident – but we will want to know the potential scope and the cause of the breach, mitigation actions we plan to take, and how we plan to address the problem.

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

The policy will also be given to third-party contractors and data processors.

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

Clinical Audit and Research

From time to time BAPAM may conduct clinical audits and work with academic institutions to collaborate on research. The use of data is outlined in our *Research Governance Policy*.

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)
Version 3.0 = April 25 2018 (C Cordeaux)
Version 3.1= October 2019 (C Cordeaux)
Version 3.2 = September 2024 (C Cordeaux)