Information Governance Policy

BRITISH ASSOCIATION FOR PERFORMING ARTS MEDICINE

CARING FOR PERFORMERS' HEALTH

Category	Policy
Summary	This policy provides an overview of BAPAM's Information Governance principles. The policy outlines how BAPAM ensures that all the information it holds is managed efficiently and securely in line with Data Protection Act 1998 and guidance from the Information Commissioner's Office. The policy applies to all personnel (Trustees, staff, clinicians and volunteers) working for BAPAM.
Valid From	1 November 2016
Version	1.0
Date of next review	November 2016
Approval Date/ via	BAPAM Board 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* *Clinical Governance policy* *Data Protection Policy* *Data Transmission Policy* *Employee Handbook* *Guidance for Handling Confidential Information when working Remotely* *Health Records Management* *Incidents* *Research Policy*
Authors	Dr Deborah Charnock, Chief Executive Dr Rebecca Whiticar, Associate Medical Director

1. Policy background and aims:

BAPAM is an employer and healthcare provider operating in the not-for-profit sector. Information is vital for efficient management of resources and plays a key part in BAPAM's service planning and delivery, performance management and overall mission.

BAPAM recognises the importance of ensuring that information in any format is managed within a robust information governance framework and in accordance with UK legislative requirements.

2. Scope:

The information covered by BAPAM's *Information Governance Policy* includes:

- Corporate governance documents including records of Trustee appointments, Board minutes, and correspondence with the Charity Commission and with legal representatives
- Commercial/business information including funding agreements, banking, salaries and contracting
- Employment records for staff including performance management, sickness and disciplinary action
- Professional records and contracts for clinicians delivering BAPAM's clinical services
- Supporter and subscriber records, including details of individual supporters/Friends, Members of BAPAM's Directory of Practitioners, and mailing list subscribers
- Healthcare Records of performers accessing BAPAM's clinical assessment services
- Clinical governance records including patient feedback and complaints, incident reporting, whistleblowing, and safeguarding cases
- Other service user records arising from Helpline contact and participation in BAPAM education and training events
- Health advice and information about BAPAM services including e-mails, telephone and fax communication, mass media information including website and social media
- Research data including data arising from collaborative research projects

For the purposes of this policy, *personal* information includes any information from which a living individual working with or supported by BAPAM can be identified, including full name and contact details.

Specific procedures for handling different types of personal information within these categories, including healthcare records, are outlined in the *Data Protection Policy* and related documents outlined on the cover sheet.

3. Responsibilities:

The BAPAM Board of Trustees has overall legal responsibility for Information Governance. The Board delegates day to day responsibilities to BAPAM's Chief Executive. These responsibilities include policy development, implementation, monitoring and effective mitigation of risks. The Chief Executive will report regularly to the Board and Medical Committee on these issues.

All BAPAM personnel, including Trustees, staff, clinicians and volunteers, are expected to adhere to BAPAM's Information Governance principles and procedures.

4. Values:

There are 5 interlinked strands to information governance:

- Openness
- Legal Compliance
- Information Security
- Quality assurance
- Training

4.1 Openness:

BAPAM recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. BAPAM supports the principles of good corporate governance, accountability, and transparency but places equal importance on security arrangements to safeguard confidential information about personnel, patients, service users and supporters, as well as commercially sensitive data.

This balance will be maintained and reviewed through regular monitoring and discussion, particularly through the Medical Committee which oversees BAPAM's clinical governance.

BAPAM only shares personal information with third parties (including other healthcare providers involved in a patient's care) with the explicit consent of the information owner. Exceptions are outlined in the *Data Protection* policy.

Non-confidential information about BAPAM and its services should be available to the public through a variety of media, in line with BAPAM's charitable mission. Similarly, BAPAM is committed to disseminating good quality information about performing arts medicine, and will share knowledge and expertise arising from best practice in research and care.

4.2 Legal Compliance:

Although BAPAM is not a statutory service provider, its Information Governance framework must incorporate legal obligations relevant to BAPAM's responsibilities and operations, specifically the Data Protection Act (1998), Charities Act (2011) and Health & Social Care Act (2008) as well as the common law duty of confidentiality and professional protocols for handling personal data.

4.3 Information Security:

BAPAM will establish and maintain policies and procedures for the effective and secure management of information assets and resources and of the flow of information into and out of the organisation.

BAPAM will undertake regular assessments and audits of its information and IT security arrangements.

BAPAM will promote effective confidentiality and security practice to its personnel through policies, procedures and training. Similarly, BAPAM will work to uphold good practice when dealing with individual contractors and stakeholders.

BAPAM has robust incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality or data security involving BAPAM personnel, service users, stakeholders and contractors.

BAPAM will establish and maintain specific policies, procedures and guidance for the use of the internet. In particular, sensitive personal data should only be sent by email or stored on remote devices if encrypted.

BAPAM will establish and maintain policy, procedures and guidance for the handling of confidential information while working off site and in particular the use of mobile devices such as smart phones, tablets, laptops etc.

4.4 Information quality assurance:

BAPAM will promote high standards of information quality and records management through its policies, procedures and training. All BAPAM personnel are expected to maintain and promote good quality information. Wherever possible, information should be assured at the point of collection.

Healthcare records will be maintained in accordance with national standards and recommended best practice. All personnel should ensure that health information is accurate, complete, timely and relevant.

BAPAM will undertake regular assessments and audits of its information quality and data management.

4.5 Training:

All BAPAM personnel are expected to have basic Data Protection awareness and to be familiar with BAPAM's policies and procedures. Data Protection training is provided on induction for BAPAM employees, and is available to other personnel as requested.

5. 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 as an employee or volunteer.
Breaches of these procedures may constitute professional misconduct and could lead to disciplinary action and termination of involvement with BAPAM.

Version 1.0 = Nov 2016 (D Charnock, R Whiticar)
Review date = Nov 2019