BRITISH MEDICAL ACUPUNCTURE SOCIETY

DATA PROTECTION POLICY

Author – Allyson Brown

To be ratified at BMAS Council – June 2018

Next review – March 2021

Version 1.1

DATA PROTECTION POLICY

This policy covers data pertaining to four groups of data subjects:

1. Members and Academic Associates of the British Medical Acupuncture Society (BMAS)
2. Non-members who have expressed an interest in the educational activities of the BMAS
3. Staff of the BMAS
4. Patients at BMAS teaching clinics.

This policy applies to all branches of the BMAS.

Operational date: 25 May 2018.

Prepared by: Allyson Brown

Draft to be approved by: the Trustees of the BMAS

Review date: 25 May 2021

Purpose

- Complying with the law
- Following good practice
- Protecting the BMAS
- Protecting staff, members, patients, course delegates, and any potential member of these groups who entrusts their personal data to the BMAS.

Principles

- To respect the individual and to prevent harm.
- To process data in a manner that is fair and legal and respects the data subject's rights
- To obtain and hold data for defined purposes and use it only in ways that are compatible with those purposes
- To hold data that is adequate, relevant, and not excessive
- To hold data that is accurate and up to date
- To hold data only for as long as is necessary
- To ensure that appropriate security is in place for the holding of data
- To comply with the rules that apply to transfer of data to overseas.

Personal data and legal basis

Definition: Information that could be used to identify and/or contact an individual or harm them.

For BMAS members and staff this would be their full name, date of birth, phone and email contacts, bank/credit card details, and members' hepatitis B blood test results. This data is held and processed on a contractual basis.

For non-members who have expressed an interest in the educational activities of the BMAS this would be their name, phone and email contacts. This data is held and processed on the basis of legitimate interest.

For patients at BMAS teaching clinics this would be as for members and staff but also include clinical records and appointment details. Clinical records are held and processed on the basis of consent, and includes special category data. Appointment details are held on a contractual basis.

Policy statement

The BMAS is committed to protecting personal data in such a way that

- the rights of the individual whose data it holds are respected
- it is open and honest with the individuals whose data it holds
- its staff are trained and supported to handle data confidently, consistently and in compliance with this policy
- it informs the Data Commissioner of any breach.

Risks

- Members: Inaccurate, insufficient or out of date data being made available to the public; data being made public without the consent of the data subject; in this case the public includes other BMAS members
- Staff: As above; in this case the public also includes other BMAS employees
- Patients: Patients' rights to privacy compromised by data being made available without consent to unauthorised parties.

Responsibilities

The trustees have overall responsibility for ensuring that the organisation complies with its legal obligations.

Data Controller

The Data Controller is the British Medical Acupuncture Society.

Data Protection Officer (DPO)

The Data Protection Officer is a senior manager or trustee.
The DPO is responsible for

- Briefing the trustees on data protection obligations
- Reviewing the data protection policy and any other related policies
- Ensuring that data protection induction and training takes place
- Advising staff on data protection issues which are less straightforward
- Handling subject access requests
- Approving unusual or controversial disclosures
- Approving contracts with data processors such as mailing houses

Locations

The management at each location where personal data is handled is responsible for its own operational procedures, provided that the Society's overarching data protection policy is adhered to. Managers will ensure that the DPO is made aware of any changes in their use of personal data that might affect the Society's notification obligations.

Staff

All staff are required to read, understand and accept all polices and procedures that relate to the personal data that they handle in the course of their work.

Enforcement

Any member of staff failing to uphold the data protection policy of the Society will be subject to sanction as described in their own contract of employment with the Society.

Confidentiality

For the purposes of this policy confidentiality applies to information about individuals and not to information about the BMAS itself nor to other organisations.

BMAS employees will have access to personal data on a 'need to know' basis. Staff responsible for processing course/meeting bookings and membership applications will have access to relevant information including name, address, telephone/email, qualifications, bank/credit card details, and in some cases blood test results of non-members and of members past, present and future.

Staff responsible for recruitment and appraisal will have access to the personal records of staff members, whilst payroll staff will have access only to the information required for this role.

Information about patients will be accessible on a 'need to know' basis, with administrative staff having access to data required for booking and billing, and only relevant staff having access to clinical records held electronically. Paper clinical records will be held in a secure lockable cabinet accessible only by clinic staff.

Personal data of any data subject will be disclosed only with the explicit permission of the data subject to whom it refers, and for a stated use. Where permission is granted it will be recorded on the data record.

In the event that permission cannot be granted or is not granted when requested but there is a compelling reason for disclosing data, the DPO (and if appropriate, the relevant director or manager) will request a decision from the President or Vice President or, in a controversial or complex situation, from a majority of the trustees.

Staff will be made aware of the Society's data protection policy as part of their induction. They will be made aware of where the policy can be viewed. If their

role requires it the policy will be covered during their training and, if appropriate, covered again during training updates. Questions about disclosure should be addressed to their line manager in the first instance and then to the DPO if needed.

Members will be made aware of the existence of the policy on joining the Society and on renewal of membership. They will be made aware of where the policy can be viewed. Renewal of membership will require renewal of acceptance of the terms of this policy.

Patients will be made aware of the existence of the policy on booking and during the consent process, and their explicit consent obtained and recorded, should disclosure of their personal data beyond the clinic be requested or recommended.

Where disclosure is not directly related to the reason for the storing of the data, written consent of the data subject should be obtained. Should this not be forthcoming but there is a compelling reason for disclosing data, the DPO will request a decision from the President or Vice President or, in a controversial or complex situation, from a majority of the trustees.

Data requests

Where a data subject requests access to data held on themselves this should ideally be made in writing by completing a Subject Access Request Form. The request will be dealt with within 28 days of receipt. Proof of identity of the data subject may be required, including photo ID, if the data subject is not known to the member of staff responding to the request. Normally there will be no charge, but if excessive administrative work is need a reasonable charge for the excess work may be made. The data subject will be made aware of this when the request is received.

Security

Data stored electronically will be held on a secure server and be password protected. Passwords must be strong and/or changed regularly. They will never be shared between staff and if data is to be viewed outside BMAS premises it will only be done so using an internet connection that is proven to be secure. Where data is being viewed in an area that is accessible to the public it must be shielded from view and/or anonymised in such a way that data subjects are not identifiable.

Data stored on paper will be kept in a lockable filing cabinet. Access will be available only for those staff members for whom it is essential. Files will never be unattended within sight or reach of persons who are not entitled to view them and filing cabinets will be locked when unattended, with the location of the key known only to staff members for whom it is essential.

An area should be made available on BMAS premises where data, be it electronic or paper, can be viewed out of sight of staff not entitled to view it.

Retention and archiving of data

Staff: Employee records will be kept open for six years after the end of their employment unless there are circumstances warranting they be kept longer. They will then be archived until the data subject's 75th birthday. This refers to paper and electronic records.

Members: Renewal of membership of the Society will be deemed to be authority to hold personal data for a further 12 months. At the time of renewal members will be invited to read this policy and to update their personal details if necessary. Should membership not be renewed the data subject will be advised that their data will be held and reviewed from time to time before being deleted.

Data subjects who are not members of the Society will be invited to opt for their details to be stored and be made aware of the purpose for which that data will be held. This data will be reviewed from time to time and the data subjects invited to opt to continue for the data to be held. This refers to paper and electronic records.

Patients: Patient data will be reviewed eight years after either discharge or when the patient last attended an appointment. Provided the record is no longer of use it will be destroyed. This refers to paper and electronic records and includes *x*-rays, scans and any other formats.

Destruction of records

Paper records will be incinerated, pulped or shredded (using a cross-cut shredder) under confidential conditions.

Electronic records will be put securely beyond use and the Society commits to permanent deletion of the information if, or when, this becomes possible.

Transmitting personal data

Unless encrypted email is used, personal data of staff, members or patients will not be transmitted by email.

Unless encryption is employed, personal data of staff, members or patients will not be transmitted by on disk, memory stick or other portable media.

Personal data of staff, members or patients will be transported on paper only under confidential conditions or by the DPO or the DPO's representative who is fully aware of the requirements for security and confidentiality.