Handling Confidential Information While Working Remotely

BRITISH ASSOCIATION FOR PERFORMING ARTS MEDICINE

CARING FOR PERFORMERS' HEALTH

Category	Policy
Version	1.0
Summary	This policy outlines BAPAM's procedures for handling confidential information when working remotely (i.e. away from the central BAPAM administration office) to ensure compliance with Information Governance policies and Data Protection legislation. It applies to all personnel (staff, clinicians, volunteers) who work for BAPAM.
Valid From	9 December 2019
Date of next review	December 2019
Approval Date/ via	Medical committee
Distribution	BAPAM clinicians email and online forum, staff meetings BAPAM website
Related Policies	*Data Protection* *Data Transmission* *Information Governance* *Incidents* *Health Records Management*
Authors	Dr Deborah Charnock, CEO Dr Rebecca Whiticar, Assoc Medical Director

1. Purpose:

This policy outlines BAPAM's governance, safety and security procedures for handling confidential information when working away from BAPAM's central administrative office in London. It applies to all BAPAM personnel (staff, clinicians, volunteers). The aim is to ensure that safe and effective working practices are employed whilst working remotely.

Enabling personnel to work remotely is key to BAPAM's operations as a national not-for-profit healthcare organisation providing services in a variety of locations and with a diverse workforce including part-time, sessional and volunteer personnel. Facilitating access to information through personal and mobile electronic devices and online systems is particularly essential for our work. However, these practices present special risks to the security and integrity of BAPAM information, and BAPAM is obliged to ensure that handling information in a remote working environment is in compliance with the Data Protection Act 1998.

From patient, staff or organisational information held on laptops or on paper, to the contact details on a mobile phone or the financial spreadsheet emailed to a home PC, the inherent risks to information used in remote working environments should be apparent to all personnel. This policy aims to provide practical advice and guidance to enable appropriate management of these risks, and should be used in conjunction with BAPAM's *Data Protection, Data Transmission* and *Confidentiality* policies.

2. Scope:

This policy applies to all BAPAM personnel – all administrative staff, clinicians and volunteers working directly for BAPAM. It is especially relevant to personnel delivering BAPAM's healthcare services at sites separate from the administrative office and clinic in London, particularly Regional clinicians and AMABO doctors.

Remote working heightens risks in a number of areas relating to information management:

- Loss of information (through error or theft, including internet hacking)
- Damage to information (including computer viruses)
- Unauthorised disclosure

In turn, this can lead to risk of:

- Breach of confidentiality/data protection
- Compromised data quality
- Personal and corporate reputation damage
- Financial costs (including ICO fines due for breaches; compensation claims)
- Disciplinary action

BAPAM personnel are required to follow the working practices contained within this document and any related documents to ensure they:

- follow the correct processes and guidelines to facilitate safe remote access to confidential information

- understand their responsibilities in terms of the safe and effective use of personal and mobile devices
- understand their responsibility in relation to information protection, including Data Protection standards and the principles of confidentiality.

3. Definitions:

Data and Information: definitions of the types of information BAPAM is responsible for are outlined in detail in the Data Protection policy. Note that all information collected and held about our performer patients (including contact details, healthcare records, correspondence) is held legally by BAPAM on their behalf under Data Protection legislation, and the terms on which we collect and use their data are outlined in our 'Patient Contract'. This information is not the property of an individual clinician or staff member. Healthcare/Medical records are considered 'sensitive' data (in legal terms) and must be afforded the most stringent protection.

Personal device: any electronic device or system that enables access to and processing of BAPAM information but which is not owned and controlled by BAPAM. This covers devices that operate within systems belonging to other organisations, as well as domestic-use devices (e.g. a family PC) and mobile devices (see below). Personal devices used to access BAPAM information pose special risks if they are also used by non-BAPAM personnel.

Mobile device: any device which renders BAPAM information portable. This may include (but is not limited to): laptops, tablets, mobile phones (Smartphones, Blackberries etc), digital recording and storage devices such as USB sticks, CDs, DVDs, etc. Mobile devices may belong to BAPAM or may fall within the 'personal devices' category.

Hard copy information: any information arising from BAPAM work that is held in a print format (paper notes, X-rays and other imaging, etc).

4. Responsibilities:

The Chief Executive has overall responsibility for Information Governance, data protection and information management systems at BAPAM.

The Chief Executive in conjunction with the Clinics Manager is responsible for ensuring that BAPAM personnel are made aware of and are complying with the policy and related documents.

BAPAM personnel are bound by the same rules of confidentiality whilst working remotely as they are when working within the central BAPAM administration office and BAPAM's secure online systems. Individual personnel are responsible for the security of any electronic and hard copy information in their care which relates to BAPAM and are required to be aware of and understand this guidance and related documents.

5. **Operational Guidance:**

5.i Hard Copy information

- BAPAM's hard copy records are stored securely at BAPAM's administrative centre and can only be accessed and distributed by authorised BAPAM personnel

- BAPAM personnel whose main base is away from the London office and clinic may hard copy healthcare records offsite provided this is justified for providing healthcare and that the information is kept secure and confidential

- BAPAM personnel should not take other forms of sensitive data (e.g. personnel records, financial documents) offsite unless authorised by the Chief Executive, Medical Director or Chairman.

- The BAPAM Team will keep a log of all personnel holding BAPAM's sensitive data offsite

- Hard copy sensitive data and confidential information arising from BAPAM work must be stored in a locked filing cabinet, even if kept at home

- All BAPAM personnel must follow a 'clean desk' policy, even if working from home

- Hard copy, sensitive data about performers should only be held for the duration of a performer's active episode of care. Original copies should be returned to the BAPAM office for filing as soon as possible using secure delivery methods, or should be destroyed using appropriate methods (see *Data Protection Policy* for retention schedules)

- The BAPAM Team can arrange for authorised, onsite shredding services to collect information from personnel based outside the London office or for secure delivery methods for returning information to the office as outlined in the *Data Transmission* policy.

- All information arising from work for BAPAM is the responsibility of BAPAM, and BAPAM may ask for it to be returned at any time.

5.ii Electronic Information:

- Access to BAPAM's electronic database and secure server is confined to authorised Admin Team members

- Authorised personnel may access BAPAM information through personal email accounts and shared workspaces using any internet connection and/or device

- Any *sensitive data* arising from BAPAM work that is transmitted, accessed, shared or downloaded electronically must be protected by reliable encryption methods (both within the BAPAM administrative system and when working remotely) as outlined in the *Data*

Protection and *Data Transmission* policies. [1] Clinicians working remotely who need to enter into email correspondence with the Team or with third parties about patient care or onward referral should access BAPAM's encryption system through the Admin team. Whilst alternative secure methods may be available (e.g. NHS.net), clinicians using them need to be clear whether they are doing this as part of the patient's care through BAPAM or as an independent practitioner or employee of another organisation - as using other systems for BAPAM work raises issues in terms of medico-legal liability and data 'ownership'. A record of all correspondence arising from a BAPAM patient's assessment must also be available within our central administrative system

- Documents containing confidential and sensitive information should only be stored on mobile or shared personal devices temporarily (e.g. for printing off or revising for the Admin Team) and should be copied to more secure storage systems and permanently deleted from the device as soon as possible. The device or the document should be encrypted to prevent unauthorised access whilst the document is in use.

- Note that 'password protection' is not the same as 'encryption', and many online products (e.g. Dropbox) do not meet appropriate security standards for sharing confidential information or sensitive data.

- Personnel should not access sensitive data or confidential information relating to their BAPAM work through online systems that are easily accessible to other, non-BAPAM users e.g. an email account that is accessible to family members on a home computer or to work colleagues on another organisation's system (e.g. a shared 'admin@...' email address).

- Personnel must ensure that their passwords for accessing confidential and sensitive BAPAM information electronically are kept secure, and that they do not use automatic log-ins such as 'remember me' facility on mobile or shared personal devices

- Personal and mobile devices must be 'locked' whenever they are left unattended

5.iii S**ecurity in transit**

Personnel should make every effort to ensure that sensitive and confidential information in any format is not misplaced, lost or stolen. They should be especially vigilant in public settings. The information should be carried as hand luggage when using public transport. BAPAM personnel must not leave notes, paperwork or mobile devices in a car overnight or for any extended period of time.

5.iv Inspection and access

BAPAM personnel are not permitted to store electronic or hard copy records away from BAPAM's central records system on a permanent basis. BAPAM is obliged to fulfil Access requests from patients and the Admin team must be able to access information centrally at short

[1] The BAPAM Admin Team use 'Egress' encryption software and are rolling out access to all personnel working for BAPAM

notice. Regulatory bodies such as the Care Quality Commission (CQC) and Information Commissioner (ICO) also have powers to inspect personal data held by BAPAM, and it is essential that information is held centrally to facilitate access and to avoid breaches in data protection standards.

6. Health and Safety

Users must adhere to risk assessments where appropriate

Laptops should generally only be used in short bursts. If the laptop is used for extended periods of time then appropriate equipment must be used in order to minimise the risk of repetitive straining injuries (RSI) or work related upper limb disorders (WRULD)

If lifting notes, safe moving and handling techniques should be employed,

7. Incident reporting

Any adverse incident involving remote working (either when working from A regional clinic or working from home) must be reported in accordance with BAPAM's incident reporting procedures. Lost and stolen devices must be reported to the Office Manager and the Chief Executive

8. Breach of Policy

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

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

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