Data Transmission Policy

BRITISH ASSOCIATION FOR PERFORMING ARTS MEDICINE

CARING FOR PERFORMERS' HEALTH

Category	Policy
Summary	BAPAM is committed to good practice in the handling of personal data and careful compliance with the requirements of the Data Protection Act. This policy outlines BAPAM's policies and procedures for transmitting confidential patient information.
Valid from	31 Oct 2013
Version	1.1
Date of next review	April 2021
Approval date/ via	Medical Committee
Distribution	BAPAM clinicians e-mail & online forum Staff e-mail and meetings Public website
Related documents	*Information Governance* Policy
Author	Dr Deborah Charnock, Chief Executive Dr Rebecca Whiticar, Associate Medical Director
Further information/contacts	

1. Background and general principles

This document sets out the security issues that BAPAM personnel (staff, clinicians, volunteers) should consider when transmitting patient data, which includes electronic methods.

BAPAM's procedures for good practice and legal compliance are outlined.

2. Related policies

This procedure specifically supports BAPAM's *Confidentiality* and *Data Protection* policies.

3. Responsibilities

The Chief Executive is responsible for:

- issuing guidance on patient data transmission
- making specific provisions for data transmission as appropriate

All BAPAM personnel are responsible for:

- ensuring transmission is to an authorised and appropriate recipient
- assessing the risks in specific instances and proposing a method of transmission
- agreeing with the recipient that the method of transmission is adequately secure
- ensuring that the transmission reaches the intended recipient.

Data protection and confidentiality breaches and 'near misses' must be reported to the Chief Executive, who will record details on the Incidents register and develop an action plan (which may include policy review, staff training and disciplinary measures - see *Public Interest Disclosures* policy).

4. Main provisions

No security measures can achieve perfect security. BAPAM is committed, however, to taking security measures appropriate to the potential risk of harm to a patient that would be posed by information falling into the wrong hands (eg. distress and breach of confidentiality). The types of patient information, level of risk and appropriate methods for transmission are outlined below.

4.1 Types of patient data and risk

4.1.1 Patient names

Names on their own may not be especially confidential, unless there is other data associated with them or the individual is well known. Generally, sending such information is regarded as **low risk**.

However, BAPAM's *Patient Contract* gives an undertaking not to identify any individual as a BAPAM patient, and some protection when transmitting names should be considered.

4.1.2 Patient contact details

Contact details (especially residential address and mobile phone numbers) must be treated as confidential, since they may pose a risk in the wrong hands.

Sending these details should be considered **medium risk.**

4.1.3 Medical details and records

Medical details (including front sheets, clinical correspondence, consultation notes, test results etc) are highly confidential and potentially harmful to patients in the wrong hands.

Sending these details should be considered **high risk.**

4.2 Key security principles & Technical options

BAPAM has identified a range of options for transmitting patient information as appropriate to level of risk, whilst also aiming to avoid an unnecessary administrative burden or delay to patient care.

4.2.1 Hard copies

Surprisingly few postal items go missing and standard post is considered a relatively secure method for transmission of patient data, particularly for low and medium risk information. BAPAM personnel may also use it for High Risk transmissions.

However, a consideration is that if hard copy information goes missing, it is instantly accessible to anyone who gets hold of it.

Note that premium postal services add little extra protection: e.g. 'Special Delivery' is tracked en route and receives some special handling, but its main benefit is compensation for lost items, not security.

Courier services are not necessarily more secure than ordinary post, and the same safeguards apply.

To maximise security, a hard copy item for post or courier should always be prepared as follows:

- placed in a well-sealed envelope
- addressed to a named person
- address should be checked as accurate and up to date
- a return address must be included on the outside of the envelope (and the name of the sender if it is not franked through the BAPAM office)
- correct postage must be paid
- if hand delivered, the identity of the receiver must be verified

Hard copies of patient records being transported by personnel between the BAPAM admin office and clinic location (e.g. regional clinic) must be protected in standard issue 'Confidential documents' bags with coded locks. Only authorised personnel will have access to codes.

The Office and Clinics Manager is responsible for all procedures and guidance relating to transport of clinical notes.

4.2.2 Fax transmission

All patient information, including high risk, may be faxed using 'safe haven' procedures as follows:

- The sender should contact the intended recipient by phone and check the fax number

- The recipient should be standing by the receiving fax machine
- A test page should be sent and the recipient should confirm its arrival by phone/text
- Full document should be sent to the same fax number (using immediate redial where possible)
- The recipient should confirm that the full document has been received, and should not leave the fax machine until the transmission has been successfully completed

This should be done every time, even with fax numbers that have been successfully used in the past.

4.2.3 E-mail

a) Egress encryption system

BAPAM's preferred method for transmitting patient data by e-mail is an encryption product - Egress. Egress is appropriate for all levels of information risk, and both the body of the message and any file attachments are automatically encrypted.

BAPAM staff have Egress software installed on their computers which is integrated into their e-mail system. Authorised recipients (e.g. BAPAM clinicians and other healthcare professionals) of information from a BAPAM-Egress account can access the encrypted e-mail via the Egress website. BAPAM staff are able to provide instructions.

b) *Other e-mail and electronic systems*

If it is not possible to use Egress, patient information may be e-mailed as protected file attachments.

For **Low** and **medium** risk information, simple password protection is sufficient (see below). **High risk** information must be protected with encryption.

The password or key to enable decryption should never be sent by the same channel as the data itself e.g. e-mail data recipients should receive the password by a text or phone call.

File protection methods:

- **Low/medium** risk data: in a Word or Excel file which requires a password for opening; for **high risk** data, encryption options must be used (available with most software, including Winzip)
- A password should be at least 8, but preferably 10 or ideally 12 characters, including upper and lower case, numbers, and special characters. Where possible, a separate password should be used for each document.
- before sending, check the intended recipient has been correctly identified and that their e-mail address is correct
- e-mail the document as an attachment
- text/telephone the password(s) to the recipient

*c) Additional methods for **high risk** data transmission*:

- data may be saved on an encrypted memory stick and posted as outlined in *4.2.1*.
- data should only be scanned onto electronic storage systems in accordance with data protection procedures. Scanners that transmit to unprotected e-mail addresses or other systems should not be used
- data should never be sent by text
- data should never be stored on mobile devices (smartphones, laptops)

5. Breach of Policy

All BAPAM personnel will receive a copy of this procedure and training, and will be required to comply as a condition of working at BAPAM. Breaches must be reported to the Director according o BAPAM's *Incidents* policy.

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

Version 1.0 = October 2013; Version 1.1 = March 2016 (updated by D Charnock)
Review April 2018 – version 2.0 (Claire Cordeaux)
Review April 2021