Arbor
Neurorehabilitation
Services

DATA PROTECTION ACT POLICY

Authors:	Kesta Purt and Sarah Gibbin
Date Reviewed:	May 2018
Next Review Due:	May 2021
Version:	V1

1.0 Executive Summary

Arbor Neurorehabilitation Services have a legal obligation to comply with all appropriate legislation in respect of data, information and IT Security. They also have a duty to comply with guidance issued by the Department of Health, the Health and Care Professionals Council (HCPC) and guidance issued by various professional bodies.

2.0 Policy Statement

All legislation relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to the business. This relates to roles that are reliant upon computer systems such as: patient administration/payment, purchasing, invoicing and treatment planning.

Penalties could also be imposed upon businesses for non-compliance of relevant legislation and guidance.

3.0 Purpose of the Policy

This Policy aims to detail how Arbor Neurorehabilitation Services will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 1998 and GDPR that is the key piece of legislation covering security and confidentiality of personal information.

For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced.

Legislation

The legislation listed below also refers to issues of security and or confidentiality of personal identifiable information/data.

- Data Protection Act 1998
- Access to Health Records 1990
- Access to Medical Records Act 1988

- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime & Disorder Act 1998
- Computer Misuse Act 1990
- Privacy & Electronic Communications (EC Directive) Regulations 2003

4.0 Scope of Policy

4.1 Data Protection Principles

There are eight principles of good practice within the Data Protection Act 1998. These are normally referred to as the 'data protection principles'.

Principle 1

Personal data shall be processed fairly and lawfully

Arbor Neurorehabilitation Services process data under the lawful conditions of 'contract' and 'legal obligation' (see details under Caldicott Principles below)

Principle 2

Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

Arbor Neurorehabilitation Services and all therapists undertaking work for the Partnership are registered with the Information Commissioners Office (ICO).

Privacy Policy and consent forms are in place to ensure the ongoing monitoring of data and its appropriate use.

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

This principle governs what is collected, entered, held and what information can be disclosed from those systems.

Where relevant information will be pseudoanonomised (e.g. email communication between professionals or with patient).

Specific, informed consent is required from each patient ahead of sharing information with third parties. Exceptions apply in relation to risk of harm to self of others (details in Privacy Policy).

Principle 4

Personal data shall be accurate and, where necessary, kept up to date

Accuracy of information is achieved by implementing validation routines; asking patient and professionals involved in their care to keep the business up to date with any changes to personal data.

Principle 5

Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes

The retention period for therapy records is 7 years from the completion of treatment. At this time all records, paper and electronic will be destroyed. Data concerning cognitive assessment scores are kept for 20 years.

Principle 6

Personal data shall be processed in accordance with the rights of data Subjects under this Act

The Data Protection Act 1998 gives every living person the right to apply for access to information held on them by an organisation. This is known as 'Subject Access'.

Definition of Health Records

A health record is defined as a record consisting of information about the physical or mental health or condition of an individual made by or on behalf of a health professional in connection with the care of that individual. It can be in electronic or manual 'structured' form (or both) and may include such things as hand written notes, letters, etc.

Receipt of an Application

All requests for access to health records by the patient will be discussed with Arbor Neurorehabilitation Services Partners (Sarah Gibbin or Kesta Purt) directly. In most cases paper records will be sent to the patient in a manner discussed (e.g. post, or email). Arbor Neurorehabilitation Services reserve the right to deny access should disclosure of the information cause risk of harm to the patient. In such cases the content of the record will be discussed with the patient face to face in a therapeutic manner, and in a situation within which any reaction to such information can be managed. The disclosure of the record can then be reviewed.

If the application is from a Solicitor on behalf of a patient, e.g. Litigation, the request will be completed with the informed consent of the patient. This requires the patient to review and approve all documentation before it is sent and the patient can request to redact information if it is not deemed relevant to any concerns regarding risk to self or others (see privacy policy).

Making an Application

Applications can be made directly Arbor Neurorehabilitation Services, by telephone or by email.

If the applicant does not state that information is required from a specific period of time it is usually assumed that access is require to the total health record.

There is no requirement for the individual to give a reason why they wish to access their records. The application should always contain the written consent of the patient (or their legal representatives) to the release of the information.

Withholding Information
There are certain circumstances where information can be withheld from a subject access request.

Access can be denied or limited where;

- the information might cause serious harm to the physical or mental health or condition of the patient, or any other person;
- or where giving access would disclose information relating to or provided by a third person who had not consented to disclosure.

Supplying Information
Information supplied will be provided in permanent form unless this causes 'disproportionate effort' or the patient agrees to receive it in another form, e.g. the printed version is very lengthy. The information supplied must be intelligible and any abbreviations will be explained. Additional costs entailed by Arbor Neurorehabilitation Services for undertaking this work will be discussed.

Inaccurate Information
If information recorded on the treatment record is inaccurate, patients have the right to have the information corrected. However, if the patient disputes the accuracy but the Clinician maintains the information is correct, the information will remain unchanged and a note will be added to the records recording the nature of the dispute, e.g. 'Patient Does Not Agree', etc.

Request for erasure of data
Individuals have the right to request the removal of data from the business.

The request can be denied in such circumstance when the data relates to health care.

Requests will be managed on a case by case basis and through the advice of ICO where necessary.

Access to Health Records of Deceased Persons
The Data Protection Act 1998 does not have any provision for access to the health records of the deceased.

Access under these circumstances is governed by the Access to Health Records Act 1990.

The personal representative (executor or administrator of the estate) of the deceased or any person who may have a claim arising out of the patients' death may apply for access.

Access will not be allowed if the patient indicated while alive that they did not wish to be given to a particular person.

Requests will be managed on a case by case basis and appropriate advice sought where necessary.

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Arbor Neurorehabilitation Services encompasses a range of healthcare professionals, with differing therapeutic training and orientations. The nominated data processor and controller is Sarah Gibbin. The data officer is Kesta Purt.

Risk assessments have been completed for the processing of data within Arbor Neurorehabilitation Services, and appropriate mitigating processes have been implemented. See risk assessment appendix 1.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Arbor Neurorehabilitation Services do not transfer data outside of the UK. In some cases electronic storage of notes may be undertaken, with platforms operating from non UK sources. All electronic notes storage platforms are checked for GDPR compliance.

4.2 **Caldicott Principles (September 2013). Arbor Neurorehabilitation Services adhere to the Caldicott Principles:**

Principle 1

Justify the purpose(s) for using confidential information

The lawful basis for processing data for Arbor Neurorehabilitation Services is:

1) Contract:

You can rely on this lawful basis if you need to process someone's personal data:

a. to fulfil your contractual obligations to them; or

b. because they have asked you to do something before entering into a contract (e.g. provide a quote).

The processing must be necessary. If it is possible to reasonably complete the contract without processing their personal data, this basis will not apply.

2) Legal Obligation

Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So it includes clear common law obligations.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

The processing must be necessary. If it is possible reasonably complete the contract without processing their personal data, this basis will not apply.

Principle 2
Do not use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3
Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4
Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5
Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data are made fully aware of their responsibilities and obligations to respect patient confidentiality. This is completed in practice by asking for evidence of the other parties' compliance with GDPR.

Principle 6
Comply with the law
Every use of personal confidential data must be lawful.

Principle 7
The duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

5.0 Disclosure of Personal Patient Information

There are Acts of Parliament that govern the disclosure/sharing of personal patient information – some make it a legal requirement to disclose and others that state that information cannot be disclosed. These Acts are detailed below:

5.1 Legislation to restrict disclosure of personal identifiable information

- Human Fertilization and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976

5.2 Legislation requiring disclosure of personal identifiable information

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985

- Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984

5.3 Section 29 – 'Crime & Taxation'

S29 is the exemption under the Data Protection Act 1998 that allows the sharing of personal information for the purpose of assisting in the preventing and or detection of crime.

The police are most likely to ask for release of personal information under this exemption, but requests may arise from other organizations that can rely upon this exemption because they have a crime prevention or law enforcement function; e.g. Department of Works & Pensions – Benefits Fraud Office.

They must have good reason – it does not have to be rigidly applied, but it is a good idea.

The exemption does not cover the disclosure of all personal information, in all circumstances.

It only allows release of personal information for the stated purposes and only if not releasing it would be likely to prejudice (that is, 'significantly harm') any attempt by police to prevent crime or catch a suspect.

A 'blank' copy of a 'Section 29' form called 'Personal Data Request Form' is available on request.

For every request for personal information received (and about each separate individual), the following questions will be considered:

- Am I sure the person is who they say they are? (for this reason you should not take these types of requests over the phone)
- Is the person asking for this information doing so to prevent or detect a crime, catch or prosecute an offender?
- If I do not release the personal information, will this significantly harm any attempt by the police to prevent crime or catch a suspect? (The risk must be that the investigation may very well be impeded).
- If I decide to release personal information to the police, what is the minimum I should release for them to be able to do their job?

The form should be able to answer all questions.

It is the clinician's decision to release personal information under this exemption. Even if the exemption applies, there is no obligation to release the personal information.

If there are genuine concerns about releasing the personal information (e.g. because there are other legal obligations such as the information being confidential) then the police will be requested to provide a 'court order' requiring the release of personal information.

If the court decides you should release the information, the Data Protection Act is not breached.

The patient whose information is sought should will be told about the order, unless that is not practicable or would undermine the purpose for which disclosure is sought.

The Section 29 form is the 'request in writing' and is signed by investigating officer which is usually 'sergeant' or above

Any disclosure of information will be noted in the patient's records.

The Section 29 form would not be released under a 'Subject Access Request'; unless the patient was aware of the disclosure in the first instance.

5.4 Duty of Care

Duty of care dictates that there are circumstances in which breach of patient confidentiality is required if failure to do so may cause harm to the individual or others. Further details are included in the Arbor Neurorehabilitation Services Privacy Policy.

6.0 Management of a Data Breach

A breach is defined as:-

- Any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 19981and/or the Common Law of Confidentiality.
- This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy.
- Such personal data breaches which could lead to identity fraud or have other significant impact on individuals.
- Applies irrespective of the media involved and includes both electronic media and paper records.

Any breach will be disclosed to the ICO within 48 hours.
The patient will be informed and the discussion documented.
Processes will follow the advice of ICO.

7.0 Therapy Will

In the event of the death of a member of Arbor Neurorehabilitation Services, remaining senior staff will assume responsibility for disposing of data held at that time, contact current patients and inform referrers. They will follow the data protection policy in their management of the data records. This will include the disposal of all therapy records both paper and electronic, and contact data relevant to patients and referrers.

Appendix: 1 (One)
Risks Assessment

Risk identified	Actions taken to mitigate risk	Further action needed
Access to paper records through loss or theft	Paper files kept in locked cupboard. In transport locked in car. Files only unlocked when in use, at which time personally supervised.	Adhere to actions identified at all times.
Unauthorised access to electronic records on laptop or PC by loss or theft.	Laptop kept in locked cupboard when not in use. All other times supervised. All computers are password protected. Documents produced by myself are password protected. Laptop has anti-virus and firewall software installed. Confidential patient and associate data stored on electronic notes system – Smile. If stored electronically outside of cloud, this done on encrypted hard drive.	Files sent from third parties are not always password protected Upon receipt of electronic files, these are saved to cloud based storage and e-mail deleted.
Unauthorised access to or loss of phone	Phones are password protected	Adhere to actions listed

	All associates to ensure that data wiping service is activated on phone should it be stolen.	
Unauthorised access to email through hacking.	Laptop has anti-virus software and firewall installed. Patients are informed of risks to email during consent process. Documents sent are password protected, password sent in separate email, content of email itself is kept to minimal identifiable information (e.g initials only).	No further action needed. Maintain procedures.
Unauthorised access to email through error – e.g. sent to wrong recipient	Maintain vigilance, and double check recipients before sending.	Maintain vigilance.

Appendix 2 (Two)
Definition of Terms

As determined by the General Data Protection Regulation (GDPR):

'personal data' means any information relating to an identified or identifiable person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular reference to an identifier such as a name, an identification number, location data, on online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'pseudoanonomised' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person;

'controller' means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union of Member State Law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor are authorised to process personal data;

'consent' means the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

'data concerning health' means personal data related to the physical or mental health of a person, including the provision of health care services, which reveal information about his or her health status.