Hampshire Neurological Alliance (HNA)

Data Protection Policy - 18th May 2018

Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give back to citizens control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When GDPR takes effect it will replace the data protection directive 1995 and will apply from 25th May 2018 replacing the 1998 Data Protection Act.

Hampshire Neurological Alliance Policy

The following Policy is not a definitive statement on the Regulations but seeks to interpret relevant issues where they affect Hampshire Neurological Alliance (HNA). The Regulations cover both written and computerised information and the individual's right to see such records. It is important to note that the Regulations also cover records relating to staff and volunteers.

All HNA staff, trustees and volunteers are required to follow this Policy at all times.

The Chairman of HNA has overall responsibility for data protection within HNA, but each individual who processes data is acting on the Controllers behalf and therefore has a legal obligation to adhere to the Regulations.

Definitions

Processing of Information - how information is held and managed.

Information Commissioner – formerly known as the Data Protection Commissioner.

Notification – formerly known as Registration.

Data Subject – used to denote an individual about who data is held.

Data Controller – used to denote the entity with overall responsibility for data collection and management. HNA is the entity as the Data Controller with the Chairman having delegated responsibility for the purposes of the Act.

Data Processor – any individual handling or processing data.

Personal data – any information that enables a person to be identified.

Special categories of personal data – information under the Regulations that requires the individual's explicit consent for it to be held by the Charity.

Data Protection Principles

As data controller, HNA is required to comply with the principles of good information handling.

These principles require the Data Controller to:

- Process personal data fairly, lawfully and in a transparent manner.
- Obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
- Ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held.
- Ensure that personal data is accurate and, where necessary, kept up to date.

- Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
- Ensure that personal data is kept secure.
- Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights of individuals to whom the personal data relates.

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Consent

HNA must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations personal and special categories of personal data covers information relating to:

- The racial or ethnic origin of the Data Subject.
- His/her political opinions.
- His/her religious beliefs or other beliefs of a similar nature.
- Whether he/she is a member of a trade union.
- His/ her physical or mental health or condition.
- His/her sexual life.
- The commission or alleged commission of any offence.
- Online identifiers such as an IP address.
- Name and contact details.
- Generic and/ or biometric data that can be used to identify an individual.

Special categories of personal information collected by HNA will mainly relate to service users' caring requirements. Data is also collected on ethnicity for statistical purposes on a confidential basis. Consent is not required to store such information as long as only accurate data that is necessary for a service to be provided is recorded.

As a general rule HNA will always seek consent where personal or special categories of personal information is to be held.

If it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent will be sought at the earliest appropriate opportunity.

If consent is refused by the individual, advice should be sought from the Data Controller.

Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the interface and must be recorded on or maintained with the case records:

- Face to face – by use of a pro-forma
- Telephone – verbal consent should be sought and noted on the case record
- Written / E-mail – the initial response should seek response, but consent for one purpose cannot be automatically be applied to all uses

Preliminary verbal consent should be sought at the point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record. The verbal consent needs to be recorded in the appropriate fields on the computer record or stated in the email for future reference.

Written consent is the optimum consent required, verbal is the minimum.

Specific consent for use of any photographs and or videos taken should be obtained in writing. Consent should also be sought if their name is to be published in any associated publicity. For those less than 18 years of age then parental/ guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects their support this should be discussed by the data processor with their manager at the earliest opportunity.

Ensuring the Security of Personal Information

Unlawful disclosure of personal information

- It is an offence to disclose personal information 'knowingly and recklessly' to third parties.
- It is conditional that those receiving a service from us for whom we hold personal details sign a consent form allowing us to hold such information.
- In addition, service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need to know basis, but this should always be checked before disclosure to another agency.
- Where consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission should be sought from the Chief Officer or Chair.
- Personal information should only be communicated within staff and volunteer teams on a strict need to know basis and in confidential settings.

Disposal of Scrap Paper, Printing or Photocopying overruns

Names, addresses, phone numbers and other information written on scrap paper is considered to be confidential; these need to be shredded and not kept.

Shredding should be done as soon as possible and if being transported should be carried out of sight in the boot of the car.

Computers

- Where computers are networked access to personal and special categories of personal information is restricted by password to authorised personnel only.
- Computer in public areas are positioned to minimise viewing by passers-by and every computer is locked when leaving it unattended.
- Firewalls and virus protection are employed at all times to reduce the possibility of hackers accessing our systems.
- Where documents are stored on individual computers, they are regularly backed up and held securely. Devices are password protected.
- Only relevant personnel may access the records on a need to know basis.

Direct Marketing

HNA will not share or sell its database with outside organisations.

HNA holds information on our clients, staff, volunteers and other supporters to whom we send copies of our newsletters and details of activities that may be of interest to them. Specific consent to contact will be sought from them, including which formats they prefer (e.g. mail, email, phone etc) before communicating.

The following statement is to be included on any forms used to obtain personal data:

"We commit never to share or sell your information to other organisations or businesses. You can opt out of our communications by writing to:
Hampshire Neurological Alliance, 9 Love Lane, Romsey, SO51 8DE or by sending an email to support@hampshireneural.org.uk"

Privacy Statements

Any documents which gathers personal and or special categories of personal data should contain the following Privacy Statement information:

- Who we are.
- What we will do with their data.
- Whom we will share it with.
- Consent for marketing notice if appropriate.
- How long we will keep it.
- That their data will be treated securely.
- How to opt out.
- Where they can find a copy of the full notice.

Our Policy will be published on our website.

Finance

We administer our finance system using spreadsheets. All data is stored on that software, which is held on a stand-alone computer, to which access is restricted to key personnel. We may collect and process personal information relating to people using our services in order to provide that service.

The finance spreadsheets are backed up regularly, with restricted access to key personnel.

Confidentiality

Data protection and confidentiality principles apply.

When sending emails to outside organisations care should be taken to ensure identifying data is removed and that codes are used. Confidential information should be password protected in a separate document.

Any paperwork should be treated as confidential and kept securely.

Never take more personnel data with you than necessary and make sure when you leave a client's home you have the correct documentation with you.

Retention of Records

Paper records are retained for the following periods at the end of which they will be shredded.

- Client, staff and volunteer records – 6 years
- Unsuccessful staff application forms – 6 months
- Timesheet and other financial documents – 7 years
- Employer liability insurance – 40 years

- Other documentation to be destroyed as soon as it is no longer needed
- Archived records should show the destruction date

What to do if there is a Breach

If you discover or suspect a data protection breach report it to your line manager who will liaise with the Data Controller to decide action to be taken including whether it needs to be reported to the Information Commissioner and reported to the Board of Trustees.

Any deliberate or reckless breach of this policy by an employee or volunteer may result in disciplinary action, which may result in dismissal.

The Rights of an Individual

The individual has the following rights with regards to those processing his/her data:

- Personal and special categories of personal data cannot be held without the individual's consent (however the consequences of not holding it can be explained and a service withheld).
- Data cannot be used for direct marketing if consent has been denied.
- Individuals have the right for their data to be erased and prevent processing in specific circumstances:
    - Where data is no longer necessary in relation to the purpose for which it was collected
    - Where an individual withdraws consent
    - Where the individual objects to the processing and there is no overriding legitimate interest for continuing.
    - Personal data was unlawfully processed.
- An individual has a right to restrict processing.
- An individual has a right to be forgotten
- Data subjects can request in writing via the Data Controller to see all personal data held on them. This request must be complied with within 30 days of receipt of the written request.

Powers of the Information Commissioner

- The following are criminal offences which could lead to a fine and or prison sentence:
    - Unlawfully obtaining personal data
    - Unlawfully selling personal data
    - Unlawful disclosure of personal data to unauthorised persons

Further Information

Further information is available at www.informationcommissioner.gov.uk

Address:

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF