Data Protection Policy

The Data Protection Act (2018) (DPA) and the General Data Protection Regulation (GDPR)sets out the legal requirements and duties placed on data controllers (GPSS) and data processors (anyone GPSS uses to process data on our behalf) and explains the 'information rights' held by data subjects (people we hold information about).

GPSS is required to register annually with the Information Commissioner as a Data Controller. GPSS's unique registration number is ZA508900.

The DPA sets out 6 data protection principles which describe legal requirements in relation to data processing. These principles are the key 'rules' for data handling and any processing of data which breaches one or more of the 6 data protection principles is unlawful.

Although the Data Protection Act (2018) does not apply to deceased persons, the NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive. The issues arising from the processing and provision of access to deceased persons records can be complex and where these arise advice should be sought from the data protection office info@gpss.org.uk

Under GDPR each controller of personal information must decide under what basis it is processing personal information.

Data Processing

Data processing covers the obtaining, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintaining confidence between the GPSS and its patients, staff and others with whom we deal.

The DPA requires that processing of any personal information held by GPSS must be both fair and lawful. This requires that the processing meets fair processing criteria and satisfies one or more 'conditions for processing' set out in the DPA.

To ensure 'fair processing' we must be lawful, fair and transparent about the way we will use the personal data we hold. We must demonstrate that we:

- are open and honest about our identity
- tell people how we intend to use any personal data we collect about them
- usually handle their personal data only in ways they would reasonably expect
- do not use their information in ways that unjustifiably have a negative effect on them
- - help people to understand their rights

To meet this requirement GPSS publishes a fair processing notice to inform patients about the way we handle and use their personal data. This is made available in hard copy format and published on GPSS product's web sites.

Routine data processing for the purposes of patient care will normally be conducted for a purpose that satisfies one of the processing conditions in the DPA. When sharing takes place for non care reasons (often referred to as secondary purposes) it can be more challenging to satisfy a condition for processing and demonstrate it is lawful processing. This is particularly the case when sharing sensitive information or when sharing personal information without consent.

A Data Protection Impact Assessment (DPIA) should be completed on all projects, proposals or business changes that involve personal information. This could be patient information or staff information.

Principles

We must consider data protection issues as part of the design and implementation of systems, services, products and business practices;

We will make data protection an essential component of the core functionality of your processing systems and services;

We will only process the personal data that you need in relation to our purposes(s), and that we will only use the data for those purposes;

Personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;

The identity and contact information of those responsible for data protection are available both within our organisation and to individuals;

We will adopt a 'plain language' policy for any public documents so that individuals easily understand what you are doing with their personal data;

We will provide individuals with tools so they can determine how you are using their personal data, and whether you are properly enforcing your policies; and

We will offer offering strong privacy defaults, user-friendly options and controls, and respect user preferences.

Breach of Policy and Procedure

Any breach of data protection and confidentiality can have severe implications for GPSS and where significant numbers of patients are involved, can impact on the reputation of the NHS as a whole.

Breaches of confidentiality or unauthorised disclosure of any information subject to the Data Protection Act 2018 constitutes a serious disciplinary offence or gross misconduct under the Trust Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

The office of the Information Commissioner's Office (ICO) regulates data protection and is charged with upholding individual's information rights. The ICO has a wide range of powers to enforce compliance which includes the imposition of a financial penalty of up to £20,000,000.

Staff who wish to report incidents relating to data protection and confidentiality should follow the incident reporting procedures contained in the Trust Incident Reporting Policy.

Framework

IG is the means of providing a governance framework and includes the following legislation and guidance

- Data Protection Act (DPA)2018

- General Data Protection Regulations (GDPR) 2016

- Freedom of Information Act 2000

- Environmental Information Regulations 2004

- Access to Health Records Act 1990

- Department of Health Records Management: NHS Code of Practice for Health and Social Care 2016

- Computer Misuse Act 1990

- NHS Confidentiality Code of Practice

- Common Law Duty of Confidentiality

- Fraud Act 2006

- Further guidance on information governance legislation can be found in the Department of Health NHS Information Governance Guidance on Legal and Professional obligations

Document Control

Document Title	
Originator	Raza Toosy
Approved by	Raza Toosy
Date of last Review	01/04/2021
Date of Next Review	01/02/2022

Document Review

Version	Amendment	By	Date
1.0		R Toosy	01/04/2018