High Trees Medical Centre

Information Governance under the General Data Protection Regulation Policy

Introduction and Policy Aims

From May 2018, all organisations and businesses must comply with the General Data Protection Regulation (GDPR), which consolidates the current data protection laws. Organisations that are already compliant with the Data Protection Act will remain compliant with much of the GDPR, which however, introduces additional requirements, particularly regarding information governance. This policy sets out how the clinic meets its information governance duties and responsibilities under current data legislation and the GDPR.

The policy should be used with other relevant policies on:

- Applications for Access to a Deceased Client's Care Records
- Confidentiality of patients' Information
- Protecting Personal Data under the General Data Protection Regulation, which addresses the protection of personal data
- Record Keeping
- Patients' Access to Records.

Definitions

Information governance represents the systems, policies, procedures and processes adopted by the clinic to ensure that data is always:

- obtained fairly and lawfully
- held securely and confidentially
- recorded accurately and reliably
- used effectively and ethically
- shared and disclosed appropriately and lawfully
- disposed of safely to the standards required, when no longer needed.

The policy describes how High Trees, which it keeps and to which it has access, so that the information is always held safely and securely, and is lawfully used. In carrying on its business of

providing support, care and treatment, the service will obtain and use the personal data of different groups of people: its patients and others relevant to them, its employees and others, such as contractors and suppliers of goods and services. The clinic is bound by law and its registration requirements to achieve established standards in its handling and management of information.
In addition to the record-keeping policies described above, the information governance framework includes several interrelated policies and procedures that contribute to its effectiveness. They include:

- access to employees' data
- Caldicott principles
- computer systems and internet: acceptable use
- internet use: staff
- Internet use: patients
- IT disposal
- the use of mobile telephones
- quality assurance: monitoring and reviewing the service provision
- sharing information with other providers
- social media.

Legal Requirements

High Trees recognises that information governance requirements have developed from a raft of legislation and statutory guidance, including:

- Data Protection Act 1998 and the General Data Protection Regulation, which when in force from May 2018, will effectively replace the Data Protection Act as the overriding legislation
- the Common Law duty of confidentiality as applied, for example, in the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- Freedom of Information Act 2000
- Human Rights Act 1998
- the Caldicott Report and Principles (and their application under the Office of the National Data Guardian)
- Health and Social Care Act 2008 (and regulations)
- Health and Social Care Act 2012

- Information Governance Alliance: Records Management Code of Practice for Health and Social Care 2016.

It also acknowledges the importance of complying with Regulation 17: "Good Governance" of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, which requires registered care providers to have effective systems and processes for, among other aspects of administration, keeping records on every client, maintaining records and striving for continuous improvements to their systems (see regulations 17(c), (d), and (f)).

The Information Governance Framework

Scope

The information governance framework for this clinic covers all records used for or with the care and treatment of its patients, staff records and administrative records likely to contain confidential information. All such records will be handled and kept safely, securely and lawfully to the same standards established by the Records Management Code of Practice regardless of their formats, including written records, forms, photographs, audio-visual, CCTV records, computer and smart device electronic records.

The Component Parts

The clinic recognises that it must achieve agreed standards for each aspect of its information governance system, which, following the Records Management Code of Practice and the GDPR requirements, requires attention to the following.

Records system design

Each set of records and record keeping arrangements are designed so that they are always fit for purpose (including using an appropriate format) and can be correctly handled and maintained. All features of the record keeping arrangements are kept under constant review, regularly audited and changed or replaced if they become unfit for purpose and fail to achieve the required standards.

Records handling and use

The clinic has put into place effective procedures to ensure that records storage, arrangements for authorised access, information sharing, transfer of records, and quality of recording are all maintained to the required standard as per the respective policies referred to in the *Introduction*.

Audit, review and retention

All records and record-keeping systems are regularly audited and reviewed for their current purpose and quality in line with the clinic's auditing schedules. Records that are no longer needed will be stored or archived safely and securely for the retention periods set out in the Records Management Code of Practice (Appendix 3).

Appraisal

At the minimum retention date, records will be appraised to identify if they will be required further, and if not, they will be safely disposed of. Where patients' health and social care records have been integrated (as they might in an NHS owned or commissioned facility or care home with nursing) the clinic will comply with the eight year retention period stated in Appendix 3 of the Records Management Code of Practice.

Note:

The eight-year retention period given in the Records Management Code of Practice is at variance with the three-year minimum retention period that for data protection reasons applies to care homes and domiciliary clinics, where they have independent record-keeping systems.

Disposal

The clinic will safely dispose of all records that have passed their minimum retention period and are no longer needed. The methods of safe disposal will depend on the type of record. Paper records will always be confidentially shredded and records kept of the means and date. Electronic records stored on computers, smartphones or other such devices will be disposed of using approved methods and IT expertise.

Management Responsibilities

Where responsibilities are delegated to someone other than the registered manager, the person(s) will be responsible to the registered manager, who will be responsible to the registered provider.

Every person with information governance responsibilities has clearly defined roles for ensuring the safe, secure and lawful use of the records for which they are responsible, for oversight of any or all stages of the lifecycle of the salient records from design to disposal (see above), and for maintaining standards.

Achieving, Maintaining and Improving Governance Standards

The clinic is committed to ensuring that all personal data that it creates, uses, handles and manages, achieves and maintains the highest standards of information governance possible.

The clinic considers that it will improve governance standards by, for example:

- ensuring that all staff and contractors supplying goods and services understand how to keep confidential any personal information they receive, and in line with data protection requirements
- ensuring that staff receive suitable training from induction onwards in the clinic's policies and procedures for safe handling and using information
- ensuring that all related policies and procedures on record keeping, confidentiality, consent, data protection are always adhered to by all staff, partners and stakeholders
- ensuring that all personal data in any form is kept safe and secure
- stating its commitment to continuously improving its information governance through its improvement plan.

Losses and Breaches of Information Safety and Security

The clinic will act quickly to repair and mitigate any damage or harm caused by accidental or deliberate loss of sensitive data or breaches of the established policies and procedures in the handling of the data, especially if the events are harmful or potentially harmful to its patients.

The clinic will always investigate thoroughly any loss of information or breaches in the handling of sensitive information and will fully cooperate with other organisations that might be involved in the loss or damage, including police if there is evidence that criminal acts have been committed.

Employees who fail in their duty of care to protect sensitive information will be subject to the service's disciplinary proceedings. If the service receives a complaint about the mishandling or loss of personal data, it will investigate the matter through its complaints procedures, which might also entail working with other organisations with whom the data is shared.

The clinic will also take suitable action against any third parties with access to sensitive information, who have not followed the required policies and procedures over confidentiality, etc.
In the event of individuals suffering significant harm from any personal data losses or being placed at high risk of being harmed, the service in line with its legal obligations under the GDPR inform the Information Commissioner's Office so that it can investigate.

Training

New staff are trained in the clinic's policies and procedures for record keeping, consent and confidentiality, etc as part of their induction training, which follows the Care Certificate Standards framework.
All staff can expect to receive instruction and dedicated training as needed in the service's record keeping policies and procedures.

Last reviewed 26/04/18