LANTERN HEALTH DATA PROTECTION AND INFORMATION SECURITY POLICY

Introduction

This Policy sets out how Lantern Health will deliver its duty to keep patient information safe and confidential without comprising its ability to share information where needed for patient care.

On the 1st March 2000 the 1998 Data Protection Act became law. This was replaced with the new Data Protection Act 2018, along with GDPR from May 2018. The Act replaced the 1984 Act and the Access to Health Records Act 1991 in respect of living persons and provides the legal framework to deliver the requirements of the recommendations of the Caldicott Committee.

The 2018 New Data Protection Act includes manual data if the data forms part of a paper based personal data filing system structured to specific criteria relating to individuals, allowing easy access to personal data. Sound and image data are included as are the collection, retrieval, destruction and use of such data, whether done manually or electronically. The Freedom of Information Act 2000 makes a number of amendments to the Data Protection Act 1998. One of the most significant is that the definition of 'data' is extended, as far as public authorities including all Independent Practitioners are concerned, to cover all personal information held. This will include 'structured' and 'unstructured' manual records.

The principal aim of the 2018 New Data Protection Act is to strengthen the individuals' right to privacy with respect to the processing of personal data and ensure that processing is done in accordance with the rights of the individual.

This policy applies to **all staff** including locum GPs, non-employed nursing staff, temporary staff, volunteers and contractors.

Legislation

Lantern Health will take all reasonable measures to ensure full compliance with its legal responsibilities as set out in:

- The Data Protection Act 2018
- GDPR 2018
- The Copyright, Designs and Patents Act 1988
- The Access to Health Records Act 1990
- Computer Misuse Act 1990
- The Health and Safety at Work Act 1992.
- The Freedom of Information Act 2000
- The Human Rights Act 1998

Types of Information Held by the Practice

The information held by the Practices will be adequate, relevant to its stated needs and purposes, and not excessive. It will not be held any longer than is necessary or required by law.

Sensitive Personal Data

The practice will follow conditions of the Data Protection Act 2018 when processing the following sensitive personal data:-

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership
- physical/mental health
- sexual preferences
- commission or alleged commission of offences
- criminal records or proceedings

Lantern Health will make every reasonable effort to ensure that the information it holds is accurate and up-to-date, as appropriate. It will correct any errors in the information it holds.

Disclosure of Information

- The person in charge of a patient's care, appropriate healthcare professional or senior manager is responsible for informing the patient of how their personal information will be recorded and for what purpose.

- All staff will be made aware of the type of information held about them and how it is used.

- Individuals on whom information is held will be allowed access to such data in accordance with government legislation and clinical judgment.

- Lantern Health and its employees will not disclose information to any individual or organisation that does not have the right to see it.

- The information held by the Practices will not be shared with any other parties except in accordance with the disclosure clauses set out in its formal Data Protection Registration.

- The number and type of data items which could allow identification on an individual will be reduced to the minimum essential for the purpose. Data, wherever practical, will be anonymised.

- All data flows, existing or planned, will be tested against the basic principles of good practice. Existing data flows will be reviewed annually to ensure that they remain compatible with these principles.

- Judgments regarding disclosure and information sharing will be based on a *'minimum need-to-know'* principle; the final decision will rest with the ***Caldicott Guardian.***

- Under the Data Protection Act patients and staff have the right to receive copies of any information held electronically and any manual record made about them; they also have the right to view such records. There are exclusions to this general right. Guidance will be given by the ***Data Protection Officer***. Requests to access these records are to be made to the Network Manager.

Patients Access to Records

The Data Protection Act 2018 provides the right of access to patients to their health records. All requests for access to patients' health records will be overseen by the Caldicott Guardian. The Caldicott Guardian has responsibility for patients manual (paper) health records and will liaise with staff that create both manual and electronic records. The Caldicott Guardian will ensure that the requirements of the Act are met in accordance with the Data Protection Policy (see Appendix 1).

- Requests for access to patient health records received by anyone other than the Caldicott Guardian must be date stamped and forwarded immediately. There are strict deadlines for the release of records and failure to do so could lead to court action (see Access to Medical Records Policy).

- The right of staff to see their own records is the same as for any other patients.

Disclosure to Others

The prime use of patient information is for the delivery of personal care and treatment. However the information is also needed for other purposes.

- assuring and monitoring the quality of care and treatment (e.g. through clinical audit);
- monitoring and protecting public health;
- co-coordinating NHS care with that of other agencies;
- effective health care administration, in particular; managing and planning services, contracting for NHS services, auditing NHS accounts and accounting for NHS performance, risk management, investigating complaints and notified or potential legal claims;
- teaching;
- statistical analysis and medical or health services research.

Circumstances in which it can be disclosed

- With the patient's written consent for a particular purpose.
- On a need to know basis if the person receiving the information is concerned with the patient's treatment.
- The information is to be used for one of the purposes listed above.
- The information is required by law or under a court order.
- In child protection proceedings if it can be established that the information required is in the public interest.
- Where disclosure can be justified for another purpose. This is usually for the protection of the public.

Lantern Health **must** be able to justify any decision to pass on information.

Circumstances in which it cannot be disclosed

Where a patient has expressed a wish that information be withheld:

- the consequences for their treatment (for example where non-disclosure will affect the Practices ability to work with another agency such as the Social Services Department) must be explained to the patient.
- the patient's wishes must be communicated to other staff that need to know.

Security Measures and Access Controls

Lantern Health will have appropriate security measures in place to guard against:

- *unauthorised access to, alteration, disclosure, destruction of data, and*
- *accidental loss or destruction of data*.

Lantern Health will ensure through its documented procedures that only authorised individuals can gain access to its systems and records.

Lantern Health will ensure, wherever possible, that the EMIS Number is used in place of other personal identifiers, as a means of:

    - *preserving a higher level of confidentiality for its patients and service users*
    - *reducing the risk of revealing personal data through casual prying*.

- All equipment, records and storage media will be protected from intruders, by appropriate physical and electronic security measures.
- Where possible, all fax machines used for the sending or receipt of personal/confidential data will be placed in a secure location, a *'safehaven',* to prevent casual browsing by unauthorised personnel.
- The copying, archiving or disposal of any data, electronic or paper or other media, will be treated with the same level of security and access restrictions as applied to live data.

- All paper-based records containing personal data will be shredded after use, or disposed of using the Practices channels (e.g. confidential waste disposal company) for the disposal of confidential/sensitive data.
- All electronic media will be wiped before disposal.
- Back-ups of systems and data will be taken at regular, pre-determined intervals in accordance with the written procedures for each system.
- The Practice will ensure that appropriate contingency plans are in place, tested and reviewed regularly, to enable information and systems to be restored as quickly as possible, following a system failure or theft.

Training

- All employees of Lantern Health and locum GPs, employed and non-employed nursing staff, temporary staff, volunteers and contractors will be made aware of their personal responsibility to keep up-to-date on issues of security, data protection and confidentiality, appropriate to their role.

- Lantern Health will provide regular, on-going training and awareness sessions for new and existing staff on security, data protection, Caldicott and records management.

- Lantern Health will provide advice and guidance for locum GPs, non-employed nursing staff, temporary staff, volunteers and contractors in the recording of information in paper-based records and the entry of data on computerised systems appropriate to their role.

- Live data will not be used for testing, training or demonstration purposes unless it has been transformed or scrambled to prevent identification of the individual and the contents of his/her record.

Using information in the prevention, detection & prosecution of serious crime

Lantern Health will, under special circumstances, pass on information to help tackle serious crime. This will be justified if the following conditions are satisfied:

- without the Practice's disclosure the task of preventing, detecting or prosecuting the crime could be seriously prejudiced or delayed
- the disclosure of information by the Practice will assist local partnerships to implement the provisions of the ***Crime and Disorder Act 1998***[1]
- the information released by the Practice is limited to what is strictly relevant to a specific investigation
- decisions on disclosure are based on fact, and not rumour or supposition
- Lantern Health is satisfied that the information will be treated confidentially by the third party and will not be passed on or used for any purpose other than the investigation for which it was released.

[1] Note : Section 115 of the Crime and Disorder Act 1998 provides a statutory authority which enables the disclosure of personal information to be considered whenever it is necessary or expedient to the successful implementation of the Act

Record Logs

The Caldicott Guardian will ensure that all changes to information (amendments, additions and deletions) are recorded and logged - on both computerised and paper-based systems - as a means of providing a reliable audit trail.

Procurement & Implementation of New Information Systems

When procuring new information systems and implementing new procedures, Lantern Health will actively consider the security implications and ensure that all necessary steps are taken to comply with the requirements set out in this policy.

No information will be transferred to countries outside the European Economic area without adequate data and information security protection being in place first.

Disciplinary Procedures

All suspected breaches of the Lantern Health *Data Protection and Confidentiality Policy* will be investigated and may be subject to the Lantern Health formal disciplinary procedures. Serious breaches may result in immediate suspension and dismissal.

Appendix 1

The 8 Data Protection Act Principles

The Data Protection Act specifies the following 8 principles:

1. Personal Data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions set out in schedule 2 of the Act is met. In the case of sensitive personal data, one of the conditions set out in schedule 3 of the Act must be met.

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

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

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

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

6. Personal data shall be processed in accordance with the rights of data subjects under the Act

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.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area 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.

Appendix 2

Individual rights

An individual shall be entitled at reasonable intervals and without undue delay or expense:

- To be informed by any data user whether he holds personal data of which the individual is the subject: and
- To access any such data held be a data users: and
- Where appropriate to have such data corrected or erased.

Right to receive information

A data subject can request a copy and must be informed why information is held, who it is to be disclosed to, what the data consists of, and what the source of the data was. Disclosure extends to non-automatically processed records e.g. staff records.

Right to know automatic decision processes

The logic involved in any decision, which involves automatically processed data, must be disclosed.

Right to Prevent Processing

An individual can prevent processing of data in certain circumstances, for example where it likely to cause distress. Where data is defined as sensitive personal data (including information on physical and mental health) may not be processed without consent of the data subject. There are exceptions: medical purposes being one.