ESH/POL/38317

Epsom and St Helier University Hospitals NHS Trust

# DATA PROTECTION POLICY

| | |
|---|---|
| Version: | Version 2 |
| Ratified by: | Trust Executive Committee |
| Approved by responsible committee(s) | Information Governance Committee |
| Name/title of originator/policy author(s): | Marcus Kirby, Deputy Director ICT<br>Paul Kenny, IG Manager |
| Lead Executive(s): | Peter Davies, Director of Strategy, Corporate Affairs and ICT |
| Date issued: | February 2017 |
| Review date: | February 2019 |
| Target audience: | All staff |

# CONTENTS

1. INTRODUCTION ..... 3
2. KEY AUDIENCE ..... 3
3. SUMMARY ..... 3
4. THE POLICY ..... 4
4.1. PRINCIPLE 1 ..... 4
4.1.1. Staff ..... 4
4.1.2. Patients ..... 5
4.2. PRINCIPLE 2 ..... 5
4.3. PRINCIPLE 3 ..... 5
4.4. PRINCIPLE 4 ..... 5
4.5. PRINCIPLE 5 ..... 6
4.6. PRINCIPLE 6 ..... 6
4.6.1. Subject Access ..... 6
4.6.2. Complaints ..... 6
4.7. PRINCIPLE 7 ..... 6
4.8. PRINCIPLE 8 ..... 6
5. KEY ROLES AND RESPONSIBILITIES ..... 7
5.1. Chief Executive Officer ..... 7
5.2. Head of Corporate Governance will: ..... 7
5.3. (Information Asset Administrators) and Information Asset Owners (IAO) ..... 7
5.4. Staff, volunteers, contractors, suppliers and others that have access to Trust person confidential information ..... 8
6. HOW THE POLICY WILL BE MONITORED, AUDITED AND REVIEWED ..... 8
7. Relevant Policies and Procedures relating to Data Protection ..... 8
8. Trusts Asset Management Policy Related Legislation ..... 9
9. Appenix1 ..... 10
10. Appendix 2: NDG Data Security Standards ..... 12
11. EQUALITY IMPACT ASSESSMENT FORM ..... 13

# 1. INTRODUCTION

Epsom and St Helier University Hospitals NHS Trust has a legal obligation to comply with all appropriate legislation in respect of Data, Information and Information Technology Security. It also has a duty to comply with guidance issued by the Department of Health, the NHS Executive, other advisory groups to the NHS and guidance issued by professional bodies.

The Trust needs to collect and process personal information in order to carry out its business and provide its services.

Personal information may be collected from patients, employees, volunteers and suppliers (past, present and future).

The personal information the Trust collects such as name, date of birth, address, health information, telephone numbers and email addresses (this is not an exhaustive list) must be dealt with in compliance with the Data Protection Act 1998.

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 Trust. This relates to roles that are reliant upon computer systems such as: patient administration, clinical treatment management, purchasing and invoicing. The legislation also regulates the use of manual records relating to patients, staff and others whose information may be held within the Trust.

The Caldicott principles (appendix 1) provide guidance on the use of and or transfer of personal confidential information and the key recommendation out of the 16 in the Caldicott 2 report was that: "a senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information". (Recommendation 3)
The nominated individual is known as the Caldicott Guardian.

The National Data Guardian (NDG) standards (July 2016) (appendix 2) set out 10 actions to be undertaken to assist in protecting information from loss, damage or inappropriate use.

# 2. KEY AUDIENCE

The policy applies to all Trust employees, volunteers and all partners, suppliers and service providers to the Trust. It is compulsory that all those who work for the Trust whether as an employee, a contractor or a supplier comply with this policy, related policies and sub policies and the standards, guidelines and procedures that are derived from them.

# 3. SUMMARY

This Data Protection policy sets out how the Trust will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 1998 that is the key piece of legislation covering security and confidentiality of personal information.

# 4. THE POLICY

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

## 4.1. PRINCIPLE 1

**Personal Information must be fairly and lawfully processed, processed fairly and lawfully.**

**Fair processing/ Obtaining Consent**
There is a requirement to make the general public, who may use the services of the NHS, aware of why the NHS needs information about them, how this is used and to whom it may be disclosed. The Trust will produce patient information leaflets and posters which are customised to its own use/s of patient information.

It is a requirement of the Data Protection Act 1998 that consent to disclosure information should be given on an informed basis.

However, the issue of seeking consent to disclosure is a complex one. When an individual seeks basic care or treatment from a health organisation, consent to share information is implicit in this process, for without it, the treatment outcome might be delayed or indeed, not achieved.

The aim should, therefore, be proportionality and 'balance', by taking the following action:

To seek consent to share information in non-routine, non-emergency situations.

To seek consent where information needs to be shared with agencies outside of the originating agency, i.e. a GP referring an individual to Social Services.

To seek consent where information may be for the purposes of research and/or essential staff training, unless this information is to be anonymised.

### 4.1.1. Staff

There shall be procedures to notify staff, temporary employees (volunteers, locums) etc. of the reasons why their information is required, how it will be used and to whom it may be disclosed.

### 4.1.2. Patients

Patients will be made aware of this requirement to share and how to opt out of having their information shared (where there is not a statutory duty to do so) by the use of information posters in patient waiting areas, statements in patient handbooks/on survey forms, the Trust web site and verbally by those health care professionals providing care and treatment.

## 4.2. PRINCIPLE 2

**Personal information must be processed for limited purposes**

**Registration/Notification**

All databases which hold and/or process personal information about living individuals shall be registered with the Information Services department.

A nominated person(s) (information asset owner (IAO) will be responsible for the way systems under their control process personal information.
Information Asset Administrators (IAA's) are responsible for the day to day operation of their designated systems

## 4.3. PRINCIPLE 3

**Personal information must be adequate, relevant, and not excessive**

Information collected from individuals will be complete and shall be justified as being required for the purpose they are being requested.

## 4.4. PRINCIPLE 4

Personal information must be accurate and up to date

**Accuracy/data quality**
Users of systems will be responsible for the quality (i.e. accuracy, timeliness, completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

Staff will check with patients that the information held by the Trust is kept up to date by asking patients attending appointments to validate the information held.

Staff information will be checked for accuracy on a regular basis by the HR department.

### 4.5. PRINCIPLE 5

**Personal information must not be kept for longer than is necessary**
**Retention of information**

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
Personal information will be retained in accordance with the relevant retention schedule.

The health records retention schedule will be found as part of the health records policy

### 4.6. PRINCIPLE 6

**Personal information must be processed in line with the data subjects' rights**

Personal information must be processed in accordance with the rights of the data subject.

**Individual's rights – including subject access and the right to complain**

#### 4.6.1. Subject Access

Subject access procedures whereby data subjects can request access to the information the Trust hold about them shall be document in the Trusts Health Records policy.

#### 4.6.2. Complaints

The Trust will ensure the complaints which may be received because of a breach or suspected breach of the Data Protection Act 1998 are handled correctly and in accordance with the Data protection Act and NHS requirements

### 4.7. PRINCIPLE 7

**Personal information must be secure**

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

### 4.8. PRINCIPLE 8

**Personal information must not be transferred to other countries without adequate protection**

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

# 5. KEY ROLES AND RESPONSIBILITIES

## 5.1. CHIEF EXECUTIVE OFFICER

- has overall responsibility for the Data Protection within the Trust.
- will ensure that there is always a designated Caldicott Guardian who will be a senior member of the medical staff such as a medical director.
- Own the implementation of, and compliance with, this policy is delegated to the Deputy Chief Executive Director of Performance and Finance the Head of Information Governance, Head of information security and other designated personnel.

## 5.2. HEAD OF CORPORATE GOVERNANCE WILL:

- maintain registrations
- Manage the Trust information governance committee

**INFORMATION GOVERNANCE MANAGER**

- to act as initial point of contact for any data protection issues which may arise within the Trust
- Provide advice on data protection to the organisation.
- ensure the availability of Information Governance training for all staff types including volunteers

**DIVISIONAL GENERAL MANAGER - PATIENT SERVICES**

- ensure appropriate subject access procedures are in place to deal with requests

## 5.3. (INFORMATION ASSET ADMINISTRATORS) AND INFORMATION ASSET OWNERS (IAO)

Information asset owners (IAO) are senior managers (usually at least rank of Divisional General manager) within the organisation who are responsible for ensuring that for the systems that they are responsible for personal information is processed and shared appropriately and securely in accordance with the Data Protection Act and Caldicott principles.
The day to day responsibilities for enforcing the policy will be devolved to the information asset administrators (IAA's) managers and other nominated personnel

### 5.4. STAFF, VOLUNTEERS, CONTRACTORS, SUPPLIERS AND OTHERS THAT HAVE ACCESS TO TRUST PERSON CONFIDENTIAL INFORMATION

Staff, volunteers, contractors, suppliers and others that have access to Trust person confidential information will:

Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.

Collect and process appropriate information and only in accordance with the purposes for which it is to be used by the Trust to meet its service needs and / or legal requirements.

Ensure that information is accurate and entered correctly into systems

When information is no longer required ensure it is securely destroyed in accordance with the appropriate retention schedule and the Data Protection Act. Destruction requires the authorisation of the relevant IAO.

Will ensure that no personal information is shared inappropriately or sent to other countries without adequate protection.

## 6. HOW THE POLICY WILL BE MONITORED, AUDITED AND REVIEWED

Compliance with this policy is monitored at local level and by the information governance committee which will receive reports on the systems they are responsible for that process / store personal information (timing and content as determined by the chair of the information governance committee) from information asset owners at least once every financial year (April 1st to March 31st the following year).

This policy will be the subject of a regular review by the information governance Committee which will take place at not less than at 2 yearly intervals. Earlier review may be triggered in response to feedback from training, regulatory changes or in response to critical incidents and regulatory changes

## 7. RELEVANT POLICIES AND PROCEDURES RELATING TO DATA PROTECTION

Related policies

Information Governance Policy
Information Security Policy
Freedom of Information Policy
Health Records Management Policy

Trust Mobile Computing Policy
ICT Disaster Recovery Policy
Trust Network Security Policy
IS Legal and Regulatory Compliance Policy
Trust Backup and Recovery Policy
Trust email and internet Policy Trust Malware Policy

## 8. TRUSTS ASSET MANAGEMENT POLICY RELATED LEGISLATION

This is not a definitive list:

Data Protection Act 1998 (and subsequent Special Information Notices)

Human Rights Act 1998

Access to Health records act 1990

Computer Misuse Act 1990

Copyright, designs and patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992

Electronic Communications Act 2000

Regulation of Investigatory Powers Act 2000 (& Lawful Business Practice Regulations 2000)

# 9. APPENIX1

The Caldicott principles

**The Seven Caldicott Principles**

1. Justify the purpose(s) of using confidential information.
2. Only use it when absolutely necessary.
3. Use the minimum that is required.
4. Access should be on a strict need to know basis.
5. Everyone must understand his or her responsibilities.
6. Comply with the law.
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.

The original Caldicott Report, established six principles for NHS bodies (and parties contracting with such bodies) to adhere to in order to protect patient information and confidentiality.

It is acknowledged that NHS staff have become more reluctant to share information given the potential sanctions in doing so inappropriately.

Accordingly, the government commissioned Dame Fiona Caldicott to conduct a further Information Governance Review (the "Review") which was published at the end of April 2013.

"The duty to share information can be as important as the duty to protect patient confidentiality". The Review highlights that for health professionals to act in a patient's best interest, they need to have all the available information about the patient to do so. However, it is acknowledged that current information governance provisions (or at least the interpretation of them) have led to information not being shared when it should be. Accordingly, Recommendation 2 of the Review specifically states that:

"for the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.

Further, the Review also recognises that there are certain situations when sharing of personal information is not just preferable, but vital. An example given of this is within public health medicine in order to identify people at risk during an outbreak of an infectious disease, or to carry out health improvement and research exercises.

# 10. APPENDIX 2: NDG DATA SECURITY STANDARDS

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit

4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security

6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection

7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management

8. No unsupported operating systems, software or internet browsers are used within the IT estate

9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually

10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards

## 11. EQUALITY IMPACT ASSESSMENT FORM

In order to carry out an effective impact assessment it is important to examine all available data and research so that any adverse impact on disability can be properly assessed.

| | | |
|---|---|---|
| 1. Name of function, strategy, project or policy | Data Protection Policy | |
| 2. Name, job title, department, and the telephone number of staff completing the assessment form | Paul Kenny, Information Governance Manager<br>Tel 721 2244 | |
| 3. What is the main purpose and outcomes of the function, strategy, project or policy. | Epsom and St. Helier University Hospitals NHS Trust has a legal obligation to comply with all appropriate legislation in respect of person confidential data. | |
| 4. List the main activities of the function, project/policy (for strategies list the main policy areas) | This Data Protection policy sets out how the Trust will meet its obligations in regard to data protection. | |
| 5. Who would benefit from the strategy/project/policy | All those whose personal data is held by the trust. | |
| 6. Is it relevant to:<br>- Race Relations Act<br>- Sex Discrimination Act<br>- Disability Discrimination Act<br>- Employment Equality Regulations<br>- Religion or Belief<br>- Sexual Orientation<br>- Age | <u>Yes</u><br>In that person confidential information must be protected appropriately. | <u>No</u><br><br>Not relevant |
| 7. Do you think that the function/strategy/project/ policy could have a negative or positive impact on :<br>Race<br>Disability<br>Gender<br>Religion<br>Sexual Orientation<br>Age | Overall positive affect as the policy sets out to protect person confidential information. | |
| 8. How could you minimise or improve any negative | N/A | |

| | |
|---|---|
| impact? Explain how. | |
| 9. What consultation with relevant users on this project has taken place. | Review by the information governance committee.<br>Review by the interim head of performance and information. |
| 10. If there are gaps in your consultation and research, are there any experts/relevant groups that can be contacted to get further views or evidence on the issues. Please list them and explain how you will obtain their views. | N/A |
| 11 a) Have you involved your staff in taking forward this impact assessment?<br>11 b) How have you involved the staff | N/A |
| 12. In the light of all the information detailed in this form what practical actions would you take to reduce or remove any adverse/negative impact. | N/A |

**To be signed by the Manager completing this form.**

**Signed…… Date:** 27th February 2017