Worcestershire Health and Care NHS
NHS Trust

DATA PROTECTION POLICY

Document Type	Corporate Policy
Unique Identifier	IG-002
Document Purpose	To detail how the Trust will meet its legal obligations and NHS requirements concerning data protection, confidentiality and information security standards
Document Author	Linda Biggs, Information Governance Officer
Target Audience	All Worcestershire Health and Care NHS Trust staff
Responsible Group	Worcestershire Health and Care NHS Trust Quality and Safety Committee
Date Ratified	December 2015
Expiry Date	November 2018
Equality Impact Assessment	This Policy has been screened using the Equality Duty Assessment Form and does not require a full Equality Impact Assessment

This validity of this policy is only assured when viewed via the Worcestershire Health and Care NHS Trust website. If this document is printed into hard copy or saved to another location, its validity must be checked against the unique identifier number on the internet version. The internet version is the definitive version.

If you would like this document in other languages or formats (i.e. large print), please contact the Communications Team on 01905 760020 or email WHCNHS.HACWNHSMail@nhs.net.

Version History

Version	Circulation Date	Job Title of Person/Name of Group circulated to	Brief Summary of Change
0.1	08/08/2013	Information Governance Steering Group	
1.0	22/05/2013	Quality and Safety Committee	
2.0	10/12/2015	Information Governance Steering Group	Reviewed in line with the latest Department of Health guidelines

Accessibility

Worcestershire Health and Care NHS Trust holds a contract with Applied Language Solutions to handle all interpreting and translation needs. This service is available to all staff in the Trust via a free-phone number (0800 084 2003). Interpreters and translators are available for over 150 languages. From this number staff can arrange:

- Face to face interpreting;
- Instant telephone interpreting;
- Document translation, via the Communications Manager and
- British Sign Language interpreting.

Training and Development

Worcestershire Health and Care NHS Trust recognise the importance of ensuring that its workforce has every opportunity to access relevant training. The Trust is committed to the provision of training and development opportunities that are in support of service needs and meet responsibilities for the provision of mandatory and statutory training.

All staff employed by the Trust are required to attend the mandatory and statutory training that is relevant to their role and to ensure they meet their own continuous professional development.

Contents **Page No**

1. Introduction

Worcestershire Health and Care NHS Trust (the Trust) has a legal obligation to comply with all appropriate legislation in respect of data, information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, the Information Commissioner, other advisory groups to the NHS and guidance issued by professional bodies.

2. Purpose

This policy details how the Trust will meet its legal obligations and NHS requirements concerning data protection, confidentiality and information security standards. The requirements within the policy are primarily based upon the Data Protection Act 1998.

3. Definitions

- Senior Information Risk Owner (SIRO) – A named director who has overall responsibility for information risk within the Trust
- Information Asset Owner (IAO) – Senior Managers responsible for identifying and reporting information assets/risks in their area
- Information Asset Administrator (IAA) – are operational staff that support IAOs. They ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date
- An Information Asset is a collection of information, defined and managed as a single unit so it can be understood, shared, protected and used effectively. Information assets have recognisable and manageable value, risk, content and lifecycle. They typically include information systems, databases, system documents and procedures and archive media/data
- PID – for the purpose of this document this includes any person identifiable, confidential or sensitive information
- ComputerCenter – IT Services

4. Scope

This policy covers all information processed within the Trust, including but not limited to:

- Patient information
- Personnel information
- Organisational information
- Structured record systems – paper and electronic
- Transmission of information – fax, email, post and telephone

This policy covers all information systems purchased, developed and managed by/or on behalf of the Trust and any individual directly employed or otherwise by the Trust.

5. Training

Information Governance (IG) training is mandatory for all members of staff whether they handle patient or non-patient related information. IG training includes Data Protection requirements

IG training is available online via the Electronic Staff Records (ESR) or via a classroom based training session using the Trust's IG Training Programme, which has been approved by the Department of Health. The online ESR training and Trust's IG Training Programme are constantly reviewed and updated to make sure that staff are kept informed of any new or amended legislation or best practice guidelines.

6. Responsibilities and Duties

- The Trust's Chief Executive is the Accountable Officer who has overall accountability and responsibility for Data Protection

- The Chief Executive has delegated responsibility for Data Protection to the Company Secretary

- The Director of Finance, Information and Contracting is the designated Senior Information Risk Owner (SIRO) and is concerned with identifying and managing potential or actual information risks. This includes overseeing the Trust's information security reporting and response arrangements.

- The Medical Director is the Caldicott Guardian and oversees disclosures of patient information in accordance with the NHS Confidentiality: Code of Practice.

- The Head of Information Governance is the Data Protection Lead and is responsible for:
    - ensuring that systems and procedures are in place to support the implementation of the Data Protection Act
    - acting as an initial point of contact for any data protection issues which may arise within the Trust
    - maintaining the Trust's Data Protection registration with the Information Commissioner
    - ensuring that regular training is provided to Information Asset Owners (IAO) and Information Asset Administrators (IAA)

- Managers will:
    - ensure that staff are aware of the Data Protection policy and updates in regard to any changes in the policy
    - ensure that staff undertake mandatory IG training
    - ensure that staff have access to all systems and procedures to support the policy
    - know how to deal with subject access requests for personal information
    - register information assets with the Head of Information Governance who will

maintain a log in the Trust's information asset register

- Staff will:
  - adhere to this policy
  - undertake mandatory IG training
  - ensure that all personal identifiable information is accurate, relevant, up-to-date and used appropriately
  - ensure that all personal identifiable information is kept secure at all times

7. Policy Principles

The Trust has a duty under the Data Protection Act to hold, obtain, record, use, and store all personal identifiable, confidential or sensitive data (PID) in a secure and confidential manner at all times. This applies to all personal identifiable information relating to living individuals held in manual and computerised files, such as medical records and personal files.

The Data Protection Act dictates that PID should only be disclosed on a need to know basis.

The Trust is required to register the data that it processes with the Information Commissioner, identifying the purposes for holding the data, how it is used and to whom it may be disclosed

Under a provision of the Data Protection Act an individual can request access to their personal information, regardless of the media that this information may be in. This is known as a 'subject access request'. The Trust will ensure that systems and processes are in place to process such requests in accordance with the Data Protection Act.

The Trust will ensure that the general public, staff, and patients are aware of why the NHS needs information about them, how this is used and to whom it may be disclosed by the use of Fair Processing Notices, i.e. leaflets, posters and the Trust website. Statements about Data Protection will be included on all forms requesting personal identifiable information.

The Trust will ensure that all records will be retained and disposed of in accordance with the Trust's Records Management Policy and in line with the NHS Records Management: Code of Practice, retention and disposal schedule.

The Trust will ensure that all information assets will have a designated Information Asset Owner. A list of these nominated personnel will be maintained in the Trust's information asset register.

Each Information Asset Owner will have responsibility for ensuring there is a procedure which outlines the media, frequency and retention period for back-ups of the data and programs for the systems within their control. Those systems which are administered by Computer Centre will have their systems backed up on a regular basis as defined in the IM&T Service Level Agreement.

The Trust will ensure that personal data is held securely and adequately protected from loss or corruption and that no unauthorised disclosures of personal data are made. Further details can be found in the Information Security Policy.

The Trust shall ensure that all members of staff are aware of the Trust's Code of Conduct for Employees in Respect of Confidentiality, and that they adhere to its provisions.

Personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the European Economic Area to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects. In the event that any member of staff wishes to process personal information outside of the United Kingdom, the Head of Information Governance must be consulted prior to any agreement to transfer or process information.

The Trust will investigate any complaints that are made in connection with the Data Protection Act. If the complainant is dissatisfied with the conduct of the Trust, then they should be advised to contact the Information Commissioner.

The Trust has a duty to ensure that personal information is used lawfully and that those undertaking work for the Trust do so in a lawful manner. To meet these obligations all staff employee contracts must contain clauses that clearly identify responsibilities for information governance including: data protection, confidentiality, freedom of information, records management and information security.

A failure to adhere to this policy and its associated procedures may result in disciplinary action. Under the Criminal Justice Act 2003, financial penalties could be imposed upon the Trust, and/or employees for non-compliance with relevant legislation and NHS best practice guidance.

8. Monitoring Implementation

The Trust will monitor this policy through the Information Governance Steering Group and continued compliance with the Department of Health's Information Governance Toolkit requirements.

This policy will be reviewed every three years, or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Department of Health, the NHS Chief Executive and/or the Information Commissioners Office.

Staff will be advised of this policy through 'Team Brief'. The policy will be available to all staff via the Trust's website.

9. Associated Trust Documentation

- Information Governance Policy
- Code of Conduct for Employees in Respect of Confidentiality
- Freedom of Information Policy
- Staff Guidance on Access to Health Records
- Records Management Policy

- Information Governance leaflets on Data Protection
- IG Training Programme
- Clinical Record Keeping Guidelines
- Terms & Conditions of Employment
- Information Security Policy
- Internet and Email Access Policy

10. Related Legislation and NHS Guidance

- Data Protection Act 1998
- Access to Health Records 1990
- Access to Medical Reports Act 1988
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Criminal Justice Act 2003
- Common Law Duty of Confidentiality
- Confidentiality: NHS Code of Practice
- NHS Care Record Guarantee for England
- International Information Security Standard: ISO/IEC 27002:2005
- Information Security: NHS Code of Practice
- Records Management: NHS Code of Practice
- Caldicott Principles

11. Appendix 1 – The 8 Data Protection Principles

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained 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 those purposes.

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