Trust Policy	

CONFIDENTIALITY & DATA PROTECTION POLICY

Department / Service:	Information Governance
Originator:	Head of Information, Technology and Administration
Accountable Director:	Chief Executive
Approved by:	IG & Records Management Committee
Date of approval:	31 July 2018
First Revision Due:	31 July 2021
Target Organisation(s)	Tetbury Hospital Trust Ltd
Target Departments	All
Target staff categories	All

Policy Overview:
To detail how the Trust will meet its legal obligations and contractual obligations to comply with NHS requirements for data protection, confidentiality and information security standards

Key amendments to this Document:

Date	Amendment	By:
3/15	To update policy from 2012	JJ
7/18	Policy review with amendments in line with GDPR	JJ

Trust Policy	

Contents

1. Introduction

Tetbury Hospital Trust Ltd. (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, the Charity Commission and advisory groups to the National Health Service and guidance issued by professional bodies.

2. Purpose

This policy details how the Trust will meet its legal obligations and NHS commissioning requirements concerning data protection, confidentiality and information security standards. The requirements within the policy are primarily based upon the Data Protection Act 2018, and the General Data Protection Regulation.

3. Scope

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

- Patient information
- Personnel information
- Organisation 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.

4. Definitions

4.1 Senior Information Risk Owner (SIRO)

A named director who has overall responsibility for information risk within the Trust, within Tetbury Hospital Trust this role sits with the Chief Executive Officer

4.2 Information Asset Owner (IAO)

Senior Managers responsible for identifying and reporting information assets/risks within the Trust

4.3 Information Asset Administrator (IAA)

Are operational staff that support IAOs. They ensure that policies and procedures are followed, recognised actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date

4.4 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, database, system documents and procedures and archive media/data

4.5 Personal Identifiable Data (PID)

For the purpose of this document this includes any person identifiable, confidential or sensitive information

5. Responsibility and Duties

5.1 The Board of Trustees

The Board of Trustees is accountable for Information Governance and compliance to the Data Protection Act

5.2 The Chief Executive

The Chief Executive is the Accountable Officer and has overall responsibility for Data Protection. This position is also the designated Senior Information Risk Owner (SIRO) whose function is to identify and manage potential or actual information risks. This includes overseeing the Trust's information security reporting and response arrangements.

5.3 The Medical Director

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

5.4 The Head of Information, Technology & Administration

The Head of Information, Technology & Administration is the Data Protection Lead, and Information Governance 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 and maintaining the Trust's Data Protection registration with the Information Commissioner. Ensuring that regular training is provided.

5.5 Departmental Managers

Departmental Managers will ensure that staff are aware of the Data Protection policy and updates in regard to any changes in the policy and complete the mandatory Information Governance training annually.

They will ensure that staff have access to all systems and procedures to support the policy and know how to deal with subject access requests for personal information. They will also register information assets with the Head of Information, Technology and Administration who will maintain a log in the Trust's Information Asset Register, held with the Trust's Risk Register

5.6 Employee /workers/contractors/temporary staff including Agency

Employees, workers, contractors, temporary staff including agency will adhere to this policy. Employed staff will undertake mandatory IG training, contractors, workers and temporary staff will evidence Information Governance training.

Whilst undertaking their role they will ensure that all personal identifiable information is accurate, relevant, up to date and used appropriately and is kept secure at all times.

6. 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 Tetbury Hospital Trust Ltd and 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, NHS clinical medical notes will be retained and disposed in accordance with the NHS Records Management: Code of Practice, retention and disposal schedule.

Consultant Private Patient's medical records are not stored on site, safe storage, retention and disposal is the responsibility of the consultant undertaking the procedure/consultation. The Trust will hold PID for private patients in the theatre register, TRAK and on the patient tracking form. We do hold medical records for private GP patients and are stored in line with our records management policy.

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 the Trust will have their systems backed up on a regular basis, and in partnership with CITS 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 Trust Information Security Policy.

The Trust shall ensure that all members of staff are aware of the Trust's Confidentiality and data protection, 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,

Technology & Administration must be consulted prior to any agreement to transfer or process information.

This policy also covers corporate confidentiality and data protection, information pertaining to the business, the finances and contracts must not be disclosed without the knowledge and approval of the Chief Executive, or the Board of Trustees

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, or the Health and Social Care Ombudsman.

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 staff are required to refer to the Information Governance policies folder, which includes information security. Leaflets and posters are displayed regarding security of data and data sharing.

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.

7. Implementation

Staff will be advised of this policy through departmental team meetings. The policy will be available to all staff via the Trust's shared drive, or in paper format from the CEO office.

8. Monitoring and compliance

The Trust will monitor this policy through the Information Committee 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.

9. Associated Trust Documentation

- Information Governance Policy
- Freedom of Information Policy
- Records Management Policy
- Information Governance leaflets on Data Protection
- IG training programme
- Job descriptions
- Tetbury Hospital Trust – Information Security Policy
- Tetbury Hospital Trust – Communications Policy

10. Related Legislation and NHS Guidance

- Data Protection Act 2018
- 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

References:
Information Commissioners Website and templates:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Appendix 1 – The 7 Principles of the GDPR/Data Protection Act 2018

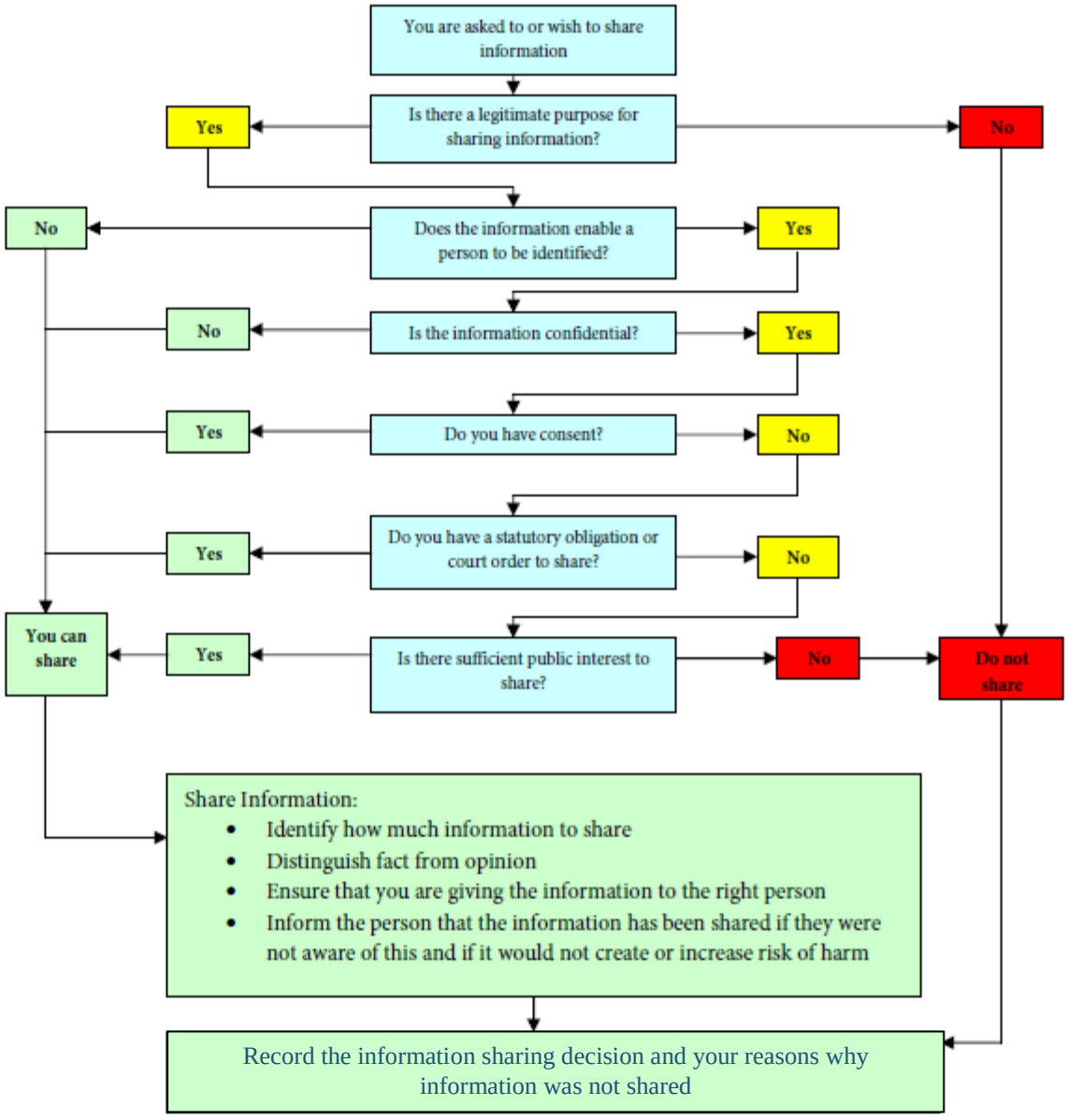
- Lawfulness, **fairness** and **transparency**.
- **Purpose** limitation.
- Data minimisation.
- **Accuracy**.
- Storage limitation.
- **Integrity** and **confidentiality** (**security**)
- **Accountability**.

Appendix 2 – Flow chart of the key principals for information sharing (Clinical)

There are occasions when information is requested, or you feel it needs to be shared (Cauldicott Principal 7)

If in doubt always seek advice from the Trust's Safe Guarding Lead, Matron Gina Ellis or, the Trust's Cauldecott Guardian, Medical Director, Mr Michael Rigby.

The reason for sharing information must always be recorded in the patients' medical record, or in the case of Safe Guarding within the designated file within the Minor Injuries Unit



Supporting Document 1 - Equality Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race		
	• Ethnic origins (including gypsies and travellers)		
	• Nationality		
	• Gender		
	• Culture		
	• Religion or belief		
	• Sexual orientation including lesbian, gay and bisexual people		
	• Age		
2.	**Is there any evidence that some groups are affected differently?**		
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**		
4.	**Is the impact of the policy/guidance likely to be negative?**		
5.	**If so can the impact be avoided?**		

6.	**What alternatives are there to achieving the policy/guidance without the impact?**		
7.	**Can we reduce the impact by taking different action?**		

Supporting Document 2 – Financial Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional Capital resources	
2.	Does the implementation of this document require additional revenue	
3.	Does the implementation of this document require additional manpower	
4.	Does the implementation of this document release any manpower costs through a change in practice	
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	
	Other comments:	

Supporting Document 3 – Privacy Impact Assessment Tool

Please review the question below: Answering 'yes' to any of these questions is an indication that a PIA is required

	Title of document:	Yes/No
1.	Will the policy involve the collection of new information about individuals?	
2.	Will the policy compel individuals to provide information about themselves?	
3.	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
4.	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used for?	
5.	Does the policy involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition	
6.	Will the policy result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	
7.	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private?	
8.	Will the prolicy require you to contact individuals in ways which they may find intrusive?	
	Comments:	

Supporting Document 4

Data Protection Impact Assessment

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA