Trust Policy	

Information Governance Policy

Department/Service:	Corporate
Originator:	Information Governance Lead
Accountable Director:	Chief Executive
Approved by:	Board of Trustees
Date of approval:	29/01/2019
Revision due:	January 2022
Target Organisation(s)	Tetbury Hospital Trust Ltd
Target Departments	All Departments
Target staff categories	All staff

Policy Overview:
The Trust recognises the importance of information, both in the terms of the clinical management of individual patients and the efficient management of services and resources. Information Governance plays a key part in supporting clinical governance, service planning and performance management. It also gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

Key amendments to this Document:

Date	Amendment	By:
September 14	First Draft	Jane Jones
08/18	Revision and update	JJ
9/20	COVID 19 – Telephone/virtual consultations – DPIA added to appendix	JJ

Trust Policy

Contents page:

1. Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning, performance and business management

It is therefore of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures and management accountability and structures provide a robust framework for information governance

Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the Trust. Senior leadership through the appointment of a Board level Senior Information Risk Owner (SIRO) demonstrates the importance of ensuring information governance remains high on the Board agenda

This policy gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible patient care

2. Scope of this document

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.
Processing within the context of this policy means any activity performed on information:

- Holding
- Obtaining
- Recording
- Using
- Storing
- Disclosing/Sharing

This policy covers all aspects of handling information within the organisation, including but not limited to:

- Patient/Service User information
- Personnel information
- Organisational information

3. Definitions

IGC	**Information Governance Committee** Forum to discuss/agree all information Governance issues and policies.
PID	**Person Identifiable Data** This is information/data about a person which would enable that person's identity to be established by one means or another. Name and address are very strong identifiers, particularly when available together.
SIRO	**Senior Information Risk Owner**

	Named director who has overall responsibility for information risks within the Trust
Caldicott Principles	A set of principles that apply to all confidential information

4. Responsibility and Duties

4.1 The Trust Board is to approve the Trust's policy in response of information Governance, taking into account legal and NHS requirements. This role may be delegated to an appropriate sub-committee or executive director. A member of the trust board will Chair the IG & Records Management Committee.

4.2 The Senior Information Risk Officer (SIRO) will be the Chief Executive. The SIRO is expected to understand how the strategic business goals of the Trust may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accountable Officer on the content of their annual Statement of Internal Control (SIC) in regard to information risk

4.3 The SIRO will provide an essential role in ensuring that identified information threats are followed up and incidents managed. They will also ensure that the Board and the Accountable Officer are kept up to date on all information risk issues. The role will be supported by the, Caldicott Guardian, and the Information Governance lead.

4.4 The Caldicott Guardian/function is supported by the Information Governance Lead

4.5 The Information Governance Lead is responsible for identifying any resources required for year on year improvements identified in the IG action plan.The Information Governance Lead is responsible for overseeing day to day information governance issues; developing and maintaining policies, standards, procedures and guidance

4.6 The Data Protection Officer Our DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits. The DPO reports directly to the highest level of management and is given the independence to perform their tasks. .

4.7 The Information Governance Committee is responsible for raising awareness and coordinating information governance across the Trust

4.8 All Managers within the Trust are responsible for ensuring that the policy and supporting standards and guidelines are built into local processes to ensure on-going compliance

4.9 All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

5. Information Governance Policy Details

5.1 Principles

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information

The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest. Please find link to GISPA – Gloucestershire Information Sharing Partnership Agreement: https://www.gloucestershire.gov.uk/council-and-democracy/data-protection/information-sharing/signa-tories-to-gispa-version-40/ Tetbury Hospital Trust is also part of the Avon IM&T Group.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such, it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision-making processes.

There are four key interlinked strands to this Information Governance Policy:

- Openness and Transparency
- Legal Compliance
- Information Security
- Quality Assurance

This high level policy is underpinned and supported by the various Trust policies mentioned in this document.

5.2 Openness and Transparency

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the Data Protection Act.

Non-confidential information on the Trust and services will be available to the public through a variety of means, in line with the Trust's code of openness and compliance with the Freedom of Information Act.

Patients will have access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from patients and the public.

The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.

Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

The Trust regards all personal identifiable information relating to patients as confidential. Compliance with legal and regulatory frameworks will be achieved, monitored and maintained.

The Trust regards all personal identifiable information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

5.3 Legal Compliance

The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements by means of the Information Governance Toolkit.

The Trust will establish and maintain policies and procedures to ensure compliance with the Data Protection Act, Human Rights Act, Freedom of Information Act and the common law duty of confidentiality.

The Trust has established and will maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act

The Trust has a comprehensive range of policies supporting the information governance agenda; reference is made to these within this policy. Legal and professional guidance should also be considered where appropriate.

5.4 Information Security

The Trust, in conjunction with Countywide IT Services Gloucestershire Hospitals NHS Trust Foundation, will establish and maintain policies for the effective and secure management of its information assets and resources.

The Trust, in conjunction with CITS, will undertake or commission annual assessments and audits of its information security arrangements.

The Trust will promote effective confidentiality and information security practices to its staff through policies, procedures and training.

The Trust will use the incident reporting procedures to monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

Information assets and information flows will be mapped and recorded to assess and prevent the unlawful and unnecessary use of Person Identifiable Information (PID)

5.5 Information Quality Assurance

The Trust in conjunction with GHNHSTF will establish and maintain policies for data quality and the effective management of records, corporate and clinical records.

Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

Department heads and leads will be expected to take ownership of, and seek to ensure their service is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness.

Wherever possible, information quality will be assured at the point of collection.

The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements by means of the Information Governance Toolkit

The Trust will promote Data Quality through policies, procedures, awareness and training.

5.6 Year on Year Improvement Plan and Assessment

The Improvement plans are aligned with the requirement of the NHS Operating Framework specifically meeting the national expectations defined in the Informatics planning guidance, these include;

- Continuing to demonstrate compliance with the key IG standards through achievement of at least level 2 performance in terms of the NHS IG Toolkit and ensuring plans are in place to progress beyond this minimum where it has been achieved;
- Ensuring that action plans for achieving the minimum of level 2 performance against all remaining requirements are already in place and are implemented by 31st March 2015.
- Mandating all staff to complete basic IG training annually appropriate to their role through e-learning.
- Continuing to report on the management of the information risks in statements of internal controls and to include details of data loss and confidentiality breach incidents in annual reports;
- Ensuring an IG audit utilising the centrally provided audit methodology is included within each organisation's auditors work plan.
- A baseline assessment will be completed at the end of November which includes the requirement to submit evidence files. A final year end assessment will be completed at the end of March each year.

6. Implementation

6.1 Plan for implementation

The Trust will ensure the policy is implemented via the Information Governance Strategy and action plan. The policy will be supported by Information Governance training, awareness and suite of policies. The Information Governance policies will be approved and

monitored by the Information Governance Committee. The overarching Information Governance Strategy and Policy will be further approved by the Trust Risk & Strategy Committee.

6.2 Dissemination

This policy will be stored on the Trust's 'shared drive'. It is the responsibility of line managers to ensure that members of staff are made aware of this policy. New members of staff are advised during their induction process to look at the Trusts Policies folder to ensure that they read and have a good working knowledge of all relevant policies, strategies, procedures and guidelines.

6.3 Training and awareness

Annual Information Governance Training is mandatory - see the Trusts Mandatory Training Matrix. The Information Governance Training and Awareness program sets out the countywide requirement for training.

Guidance for completing the Information Governance Training via https://ghft.kallidus-suite.com

The Trust's Induction programme includes guidance for staff regarding Caldicott, Data Protection and Information security. A general overview of Information Governance is provided via an IG booklet handed out at the Induction session, which raises awareness with staff and provides contact details of key personnel in all the relevant areas.

The Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs) will complete the risk management training via e-learning on an annual basis.

General awareness is conducted on a regular basis for all staff via articles in the Trust Weekly Brief.

7. Monitoring and compliance

The Trust will monitor this policy and related strategies, policies and guidance through the Information Governance Committee

As assessment of compliance with requirements, within the Information Governance Toolkit will be undertaken each year

The Information Governance Lead will monitor compliance and report progress to ensure work is undertaken to meet the requirements of the Information Governance Action Plan

Annual reports and proposed action/development plans will be presented to the Trust's Board for approval prior to submission to the Information Governance Toolkit

Internal data quality and coding audits are carried out as required. External Audits are carried out on the IG toolkit requirements on an annual basis.

Information Governance incidents are reported using an INR form and discussed weekly at the Senior Management Meeting.

The Information Governance Lead will monitor compliance with the core standards related to information governance, such as those required by the Care Quality Commission, regulation 18 and 22.

The Information Governance Lead will provide the Strategy & Risk Board sub-committee very six months on progress, development and performance of information governance in the Trust.

8. Policy Review

This policy will be reviewed biannually by the Information Governance Manager and relevant key staff.

9. References:

References:	Code:
Information Governance Strategy	
Code of Conduct for Employees in Respect of Confidentiality	
Incident Reporting Policy	
Patient Advice and Liaison Service (PALS) Policy and Procedure	
Complaints Policy	
CITS/THT Information Security Policy	
CITS/THT E-mail and Internet Policy	
THT Mobile Devices Policy	
CITS/THT User Responsibility Statement	
Data Protection Act 2018	
Freedom of Information 2000	

10. Background

10.1 Consultation

The policy has been updating by the Information Governance Lead with input from the Information Governance Committee members.

10.2 Approval process

This policy is agreed by the Information Governance Committee and then finally approved at Trust Board meeting. Minor changes can be approved by the SIRO via the IGC prior to the 2 year review.

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 any one group less or more favourably than another on the basis of:**		
	• Age	No	
	• Disability	No	
	• Gender reassignment	No	
	• Gender	No	
	• Race	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Marriage and Civil Partnership	No	
	• Pregnancy and Maternity	No	

2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	NA	
4.	**Is the impact of the policy/guidance likely to be negative?**	NA	
5.	**If so can the impact be avoided?**	NA	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	NA	
7.	**Can we reduce the impact by taking different action?**	NA	

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 – Data Protection Impact Assessment

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

	Title of document:	Yes/No
1.	Will the policy involve systematic and extensive profiling or automated decision-making to make significant decisions about people	Y/N
2.	Will the policy process special category data or criminal offence data on a large scale	Y/N
3.	Systematically monitor a publicly accessible place on a large scale	N
4.	Use new technologies	N
5.	Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit	N
6.	Carry out profiling on a large scale	N
7.	Process biometric or genetic data	N
8.	Combine, compare or match data from multiple sources	N
9.	Process personal data without providing a privacy notice directly to the individual	
10.	Process personal data in a way which involves tracking individuals online or offline location or behaviour	
11	Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them	
12	Process personal data which could result in a risk or physical harm in the event of a security breach	
13	Systematic processing of sensitive data or data of a highly personal nature	
14	Processing on a large scale	
15	Processing of data concerning vulnerable data subjects	
16	Innovative technological or organisational solutions	
17	Processing involving preventing data subjects from exercising a right or using a service or contract	

	Title of document:	Yes/No
18	Is this a major project involving the use of personal data	
	Comments: **If we decide not to carry out a DPIA we document our reasons why** **We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing**	

Data Protection Impact Assessment

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.

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.
Following government guidelines during the COVID-19 pandemic, Tetbury Hospital will be undertaking telephone consultations with both NHS and private patients. Video consultations will also be available should the need arise.

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?
The data used to conduct an NHS telephone consultation where the Consultant is remote working, will be through the Trak patient administration system. The consultant has a secure remote log-on. The consultant will be able to review referral letters, clinic details, test reports and x-rays within a secure environment. If additional information is required the secretaries will use nhs.net mail to nhs.net mail. The consultant will delete after use. Consultants will not be permitted to take any paper records off-site. If the calls are conducted off-site then electronic information should be used. There will be no data shared outside of standard processing The consultants are mainly running a telephone consultation service, but will be based within the hospital. Those that are remote working, are in fact working from GHNHSFT, so still within a secure area. Private Patients: The records for private patients are owned by the Consultants – should a telephone consultation be required the Consultant will have the patient information sent to them by their private secretary. General GDPR regulations still apply whether the calls are for NHS or private patients. Consultant to ensure the correct contact details are received and that patient is aware that a phone consultation will be taking place. Consultant to ensure the call is conducted in a confidential environment.

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?
The data held within the Trak care system does not contain special category or criminal offence data. None of the consultants have opted for video appointments – this has not therefore been set up. For private patients, the information is held/owned by the consultant, who is responsible for processing and record keeping in line with GDPR

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)?
No change to the context of processing. Consultants continue to use the patient administration system via secure link (VDI) through HSCN, but carry out telephone consultations. For private patients the information is made available to the consultants via their private secretary. The information is shared with the consultant via encrypted/password protected methods.

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?
To achieve a safe environment to treat patients both NHS and private during this pandemic. To ensure that patients at risk – such as glaucoma continue to receive a review by the consultant. By carrying out telephone consultations the patient can be triaged and advised until such time as face to face consultations return.

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?

All patients are spoken to verbally by telephone to offer this type of appointment. This is then followed up with an appointment time range, ie they will be called between 9am and 12pm. For private patients the private secretary will arrange the appointment

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?
As a charity with an NHS contract we have been authorised by the government to provide healthcare and must keep accurate records for this. Under GDPR our legal basis for processing patient information is: Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject, Article 6(1) (e) the performance of a task carried out in the public interest or in the exercise of the controller's official authority, and, Article 9(2) (h) the provision of health or social care or treatment or the management of health of social care systems and services. The above also applied for private patients.

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
Misunderstanding/ misinterpretation by patient or consultant – Patient receives a copy clinic letter	1 1	1 1	1 1

confirming discussion Missed appointment – the patient would be contacted by the booking office and rearranged.			

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**
N/A		Eliminated reduced accepted	Low medium high	Yes/no

Item	**Name/date**	**Notes**
Measures approved by:	SIRO	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	None	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Approved to go ahead		
DPO advice accepted or overruled by:	CEO	If overruled, you must explain your reasons

Comments: Accepted		
Consultation responses reviewed by:	SMT – Caldicott Guardian	If your decision departs from individuals' views, you must explain your reasons
Comments:Accepted		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA