Gloucestershire Hospitals NHS
NHS Foundation Trust

TRUST POLICY

INFORMATION GOVERNANCE POLICY

This document may be made available to the public and persons outside of the Trust as part of the Trust's compliance with the Freedom of Information Act 2000

Please be aware that only documents downloaded or viewed directly from the GHNHST Trust Policies webpage are valid documents. Documents obtained through internet searches may be out of date and therefore will be invalid

FAST FIND:

- **B0413 IG1 Action Card - Removal of Consent to use Personal Information for Non-Clinical Purposes**
- **Gloucestershire Information Sharing Partnership Agreement (GISPA)** (The Trust is not responsible for the content of external websites)
- **SUS/HSCIC Data Patient Opt-Out Form**

1. INTRODUCTION / RATIONALE

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 and performance management.

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

2. DEFINITIONS

Word/Term	Descriptor
Information Governance	Information Governance is the framework of law and best practice that regulates how information (including information relating to and identifying individuals) is managed, i.e. obtained, handled, used and disclosed.
Information Governance Assurance Framework	The Information Governance Assurance Framework (the "Framework") is a national framework of standards that bring together all statutory, mandatory and best practice requirements concerning information management. The standards are set out in the Department of Health Information Governance Toolkit (IGT) and cover the following areas: - Access to information (Freedom of Information Act 2000 and Subject Access Requests) - Confidentiality and Data Protection Act 1998 - Information security assurance - Information quality assurance - Records Management

3. POLICY STATEMENT

The aim of this policy is to brief staff on the trust's IG requirements, outline the training provision, reporting structure, risk and incident management processes and the annual IG work plan and give assurance to the Trust and to individuals that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

The policy applies to all staff whether permanent, temporary, or contracted staff, including contractors that are employed directly or otherwise by the Trust.

This policy covers all aspects of information management within the Trust, including:

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

And all aspects of handling information, including:

- Structured record systems - paper and electronic
- Transmission of information – fax, e-mail, post and telephone, removable media
- Sharing of Information to third parties

Information Governance provides a way for the Trust to deal consistently with the many different rules about how information is handled, including those set out in:

- The Data Protection Act 1998.
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice.
- The NHS Care Record Guarantee for England.
- The Social Care Record Guarantee for England.
- The international information security standard: ISO/IEC 27002: 2013 and ISO/IEC 27001: 2013.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
- The Freedom of Information Act 2000.
- The Human Rights Act article 8.
- The 'Report on the review of patient-identifiable information' (alternative title 'The Caldicott Report') and the 'Information: To share or not to share? The Information Governance Review (also known as the Caldicott 2 Review).
- Information: To share or not to share - Government Response to the Caldicott 2 Review.
- National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs (also known as Caldicott 3 Review)
- General Data Protection Regulation (GDPR)

4. ROLES AND RESPONSIBILITIES

(Including Senior Roles and Governance Framework responsibility, accountability and resources)

Post/Group	Details
Trust Board	• To approve the Trust's Policy in respect of Information Governance, taking into account legal and NHS requirements. This role may be delegated to an appropriate sub-committee or executive director. • To receive a report at least annually on the Trust's Information Governance performance.
Trust Senior Information Risk Owner (SIRO) **(Director of Clinical Strategy)**	• Named Executive Director on the Board with responsibility for Information Governance. • To undertake the role of Senior Information Risk Owner (SIRO) for the Trust • Chair of the Trust Information Governance and Health Records Committee • To appoint the Lead for Information Governance • To appoint a trust lead for Data Protection and Freedom of Information
Caldicott Guardian **(Medical Director)**	• Named Executive Director with responsibility for Caldicott and is a member and vice chair of the Information Governance and Health Records Committee.
Lead for Information Governance **(Information Governance and Health Records manager)**	• Overseeing day to day Information Governance issues • Developing and maintaining policies, standards, procedures and guidance • Co-ordinating Information Governance in the Trust and raising awareness of Information Governance • Co-ordination of the completion and annual submission of the IG Toolkit • Lead on management of Information Governance Serious Incidents requiring investigation (IG SIRI)
Lead for Data Protection and FOI	• Overseeing day to day Data Protection and FOI issues • Developing and maintaining policies, standards, procedures and guidance • Co-ordinating and raising awareness of legal compliance
Data Protection and FOI Officer(s)	• Overseeing day to day FOI and DPA access to health record issues

The Information Governance and Health Records Committee	• Accountable to the Trust Leadership Team via the Chair • Approving the results of information governance audits prior to presentation by the Trust Board
IG Standard Management Leads and Directors	• Assessing Information Governance performance against the Department for Health Information Governance Toolkit Standards • Submitting results to the Department of Health on an annual basis via the Department for Health Information Governance Toolkit as co-ordinated by the Lead for Information Governance • Responsible for cascading IG requirements within the organisation in relation to the IG Standard for which they are the lead
Managers	• To ensure that this Policy and any supporting documents are built into local processes • To ensure that the development of any new systems will be compliant with Information Governance requirements
All staff	• To ensure that they are aware of Information Governance requirements and standards including data protection responsibilities in relation to their specific role and are compliant with these standards and responsibilities • To ensure that they complete IG and Code of Confidentiality mandatory training • To report IG related incidents including data breaches through the trust incident reporting tool Datix • To escalate any IG related concerns through their Line management and / or to the IG Lead
Information Asset Owners (Heads of Department and budget holders)	• Overall responsibility for information assets in their own area, however funded. • To ensure that effective system management responsibilities are defined and that known risks are scored, recorded and escalated according to the Trust's risk management procedures.
System Managers	• To ensure that all suppliers, whether providing new systems or developing legacy systems show evidence of compliance with Information Governance by completion of the Department for Health Information Governance Toolkit for Commercial Third Parties • To submit Information Governance Systems forms when required • To provide evidence of compliance with Information Governance requirements when requested

5. 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.

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 4 key interlinked strands to the Information Governance Policy:

5.1 Openness

Non-confidential information on the Trust and its services should be available to the public through a variety of media.

- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media
- The Trust will have clear procedures and arrangements for handling queries from patients and the public

5.2 Legal compliance

The Trust regards all identifiable personal information relating to patients and staff as confidential and as such takes steps to ensure that the handling of such information complies with the Data Protection Act 1998 except where there is a legal requirement to override the Act.

- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements
- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act 1998, the common law of confidentiality and the Freedom of Information Act 2000.
- The Trust will establish and 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 2001, Crime and Disorder Act 1998, The Children's Act 2004)

5.3 Information security

The Trust will establish and maintain policies for the effective and secure management of its information assets and resources

- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Trust will maintain and review incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

5.4 Quality assurance

The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.

- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers and senior clinical staff are required to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality will be assured at the point of Collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training

6. KEY POLICIES AND PROCEDURES

A full list of policies and procedures is available on the Trust intranet site Policy Library. Including Key Information Governance policies:

6.1 Information Governance Policy B0413

To brief staff on the trust's IG requirements, outline the training provision, reporting structure, risk and incident management processes and the annual IG work plan and give assurance to the Trust and individuals that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

6.2 IT Security Policy B0591

To ensure that electronic data is protected in all of its forms, during all phases of its life cycle, from unauthorised or inappropriate access, use, modification, disclosure or destruction, through the application of the standards and definitions of the ISO27000 series of standards as used in the Department for Health Information Governance Toolkit.

The policy applies the key concepts of Information Assurance to electronic data processing in the Trust:

- Confidentiality
- Integrity
- Availability
- Accountability

6.3 Records Management Policy B0259

To ensure compliance with the legal and professional obligations set out in the Records Management:

NHS Code of Practice, in particular:

The Public Records Act 1958;
The Data Protection Act 1998;
The Freedom of Information Act 2000;
The Common Law Duty of Confidentiality;
The NHS Confidentiality Code of Practice
Including the management of access to health records requests and requests for information made under the freedom of Information Act 2000.

These and all other IG related policies are reviewed as required as part of the IG Strategy and annual improvement work plan.

6.4 The Information Governance Toolkit

The annual information governance assessment is measured against the standards set out in the Department for Health Information Governance Toolkit and is assured each year by Internal Audit. The Trust is required to submit three Information governance performance reports to the NHS Digital which can be tracked by Commissioners and other monitoring bodies. The reporting deadlines are:

- Baseline assessment (31st July)
- Performance update (31st October)
- Final submission (31st March)

The final performance assessment submitted to the NHS Digital on the 31st March is shared with the Care Quality Commission, the Audit Commission, Monitor and the National Information Governance Board. The results are also published on the NHS Digital website and made available to the general public.

6.5 The NHS Department for Health Information Governance Statement of Compliance

All organisations wishing to access and use NHS systems and services, including the N3 network, must meet the terms and conditions in the Information Governance Statement of Compliance (IGSoC). The IGSoC is the agreement between NHS and Approved Service Recipients that sets the information governance policy and terms of conditions for use of NHS services.

The IGSoC contains a number of obligations which aim to preserve the integrity of these services, which requires:

No patient identifiable data or other sensitive data is stored or processed offshore, where the location is deemed non-compliant with the NHS Offshore Policy

- The right of audit by NHS Digital or nominated third parties
- Change Control Notification procedures and approval processes
- Organisations to achieve or be working towards ISO27001
- Organisations report security events and incidents

6.6 Privacy Impact Assessments

The impact of any proposed changes to the Trust's processes and/or information assets need to be assessed using a Privacy Impact assessment template. Used for large scale change, discussion

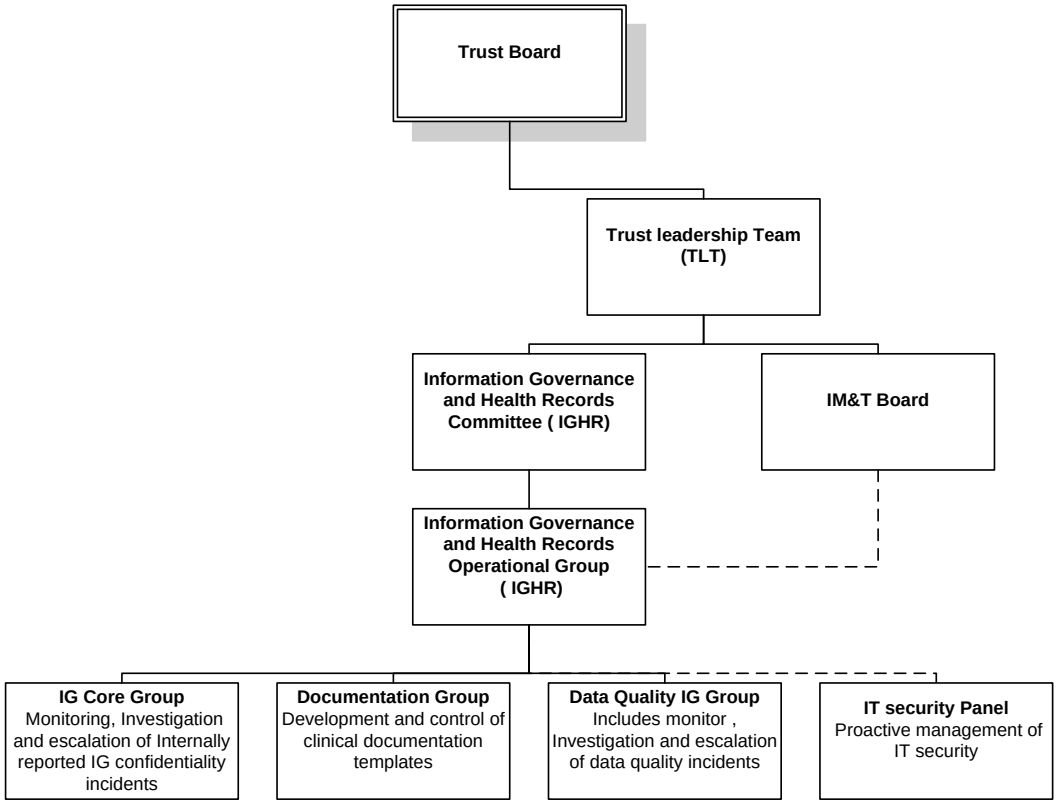
underway to plan how to roll out practice further, to ensure that the confidentiality, integrity and accessibility of personal information is maintained.

6.7 Information Asset Register

The Trusts information Asset register is currently maintained in two sections;
Electronically held information assets are managed as part of the Critical systems log reviewed and maintained by the IM&T Board and include business continuity and IT support information
Paper based records on the separately held subsidiary records log

7. KEY GOVERNANCE BODIES

Information Governance Committee Reporting Structure



7.1 Information Governance and Health Records Committee (IGHR)

The IGHRC has responsibility for overseeing the implementation of this Information Governance Policy and Framework, the annual information governance toolkit assessment and the annual Information Governance improvement plan. This Committee also reviews and approves all IG-related policies and procedures.

7.2 Information Governance and Health Records Operational Group

The work of the IGHR is supported by an Information Governance and Health Records Operational Group which is the basis for the Information governance team within the trust, with representatives from all clinical, divisional and specialist areas including subject matter expert leads for the IGT standards

7.3 IG Core Group

The group meets bi monthly for monitoring, investigation and escalation of internally reported IG confidentiality incidents on risk management system

7.4 Data Quality IG Group

The Group meets quarterly to report on ongoing monitoring, investigation and escalation of data quality incidents

7.5 Documentation Group

Control panel for the development and control of clinic document templates

7.6 IT Security Panel

Proactive management and development of IT security

8. TRAINING

Success in achieving compliance to the standards set out in the IG Framework is dependent on developing an Information Governance aware and knowledgeable work force.

Information Governance Training is incorporated into the Trust's Mandatory Training programme. It is a mandatory requirement for all GHNHSFT staff without exception to undertake annual Information Governance training which is appropriate to their role. Different levels of training need to be completed by staff, as part of their mandatory training, depending on role and is viewable through the online training matrix.

All staff receive Information Governance awareness training as part of their corporate induction programme.

In subsequent years staff complete either a basic level training or a more advanced training depending on their job role.

This is currently under review with an additional tier being considered. In addition better links from the trust mandatory training system to the online national NHS Information Governance Training Tool are being explored. The SIRO will ensure that the necessary training or education needs and methods required to implement this policy are identified and resourced or built into the delivery planning process. This may include identification of external training providers or development of an internal training process.

The training required to comply with this policy is e-Learning modules as defined by the Information Governance Committee.

9. INCIDENT MANAGEMENT

The Trust has an electronic reporting system for all incidents including IG related incidents and also offers a hotline number for anonymous reporting. IG confidentiality incidents are reviewed at the bi monthly IG core subgroup, where any required IG team support and intervention is made.

B0393 - Incidents - Managing, Reporting and Reviewing of Incidents / Accidents, including Serious Incidents

The Trust Incident Reporting System is designed to notify the Trust IG Lead and other members of the IG core subgroup of all occasions where information breaches are reported by trust staff members. This informs the scheduled meeting of the group of issues to be reviewed and also allows for more immediate action where this is required. This is in addition to the local management of incidents by the department or service lead where the incident has occurred.

IG incidents are assessed using the criteria set out in the HSCIC document; Checklist Guidance for Managing and Investigating Information Governance and Cyber security Serious Incidents Requiring Investigation. (HSCIC 2015) If confirmed as an IG SIRI, they are then graded using the same guidance and reported to the ICO via the incident reporting section of the Department for Health Information Governance Toolkit. All incident trends and IG SIRI level one or above are also escalated to the IGHR Specialist group and Committee via a bi monthly report, for further management, dissemination and escalation.

10. MONITORING OF COMPLIANCE

The SIRO, as sponsoring director, will agree with the Information Governance and Health Records Committee a method for monitoring the dissemination and implementation of this policy.

Do the systems or processes in this document have to be monitored in line with national, regional or Trust requirements?	YES

Monitoring requirements and methodology	**Frequency**	**Further actions**
Data quality Audit Data Quality Team	Annually	Reported to IGHR Committee
Legal Compliance Report Lead for Data Protection and FOI	Annually	Reported to IGHR Committee Subject to ICO action dependent on severity of non-compliance
As an Acute Trust we are required to achieve a minimum level 2 against all 45 requirements identified in the Information Governance Toolkit.	Annually	The Trust's information governance performance is measured through the baseline, improvement and annual IG Toolkit reports and reported to the Information Governance and Health Records Committee (IGHR). It is included in the trusts Quality report and a final position paper is submitted to the Trust board prior to final submission each year.
Incidents reported on Datix monitored IG Core Group (Sub-committee)	Bi-monthly	IG SIRI escalated
IG SIRI monitored within datix incidents as above, escalated to SIRO and reported in addition via IG Toolkit incident reporting tool	Annually and at time of incident	Reported to IGHR Committee, Annual IG trust board report and section included in the Trust Quality Report. Level 2 + incidents reported to ICO and NHS England through IGT. Subject to ICO action dependent on severity
IT Security Incidents Audit, IM&T Programme Manager	Annually	IM&T Board
Essential Standards of Quality and Safety The Care Quality Commission (CQC) will cross-check the Trust's Information Governance Toolkit submission as part of the assurance that the Trust is meeting the essential standards of quality and safety. This is measured against Quality and Risk Profiles and Key lines of enquiry including.	Annually	Reported through the Quality Standards Review Group

11. REFERENCES (The Trust is not responsible for the content of external websites)

Caldicott, 2013 Information: To share or not to share? The Information Governance Review Williams Lea for the Department of Health

Department of Health Informatics Directorate, 2011 NHS Information Governance Guidance for NHS Boards: Information Governance Department of Health

General Medical Council, Confidentiality, 2009 accessible via www.gmc-uk.org/guidance.

Health and Care Professions Council, 2008 Confidentiality – guidance for registrants accessible via www.hcpc-uk.org

Health and Social Care Information Centre, 2013 A guide to confidentiality in health and social care: references Treating confidential information with respect Version 1.1 HSCIC

Health and Social Care Information Centre, 2015 Checklist Guidance for Managing and Investigating Information Governance and Cyber security Serious Incidents Requiring Investigation Version 5.1 HSCIC

Information Commissioner's Office, (n.d.) Data sharing code of practice accessible via ico.org.uk

Cabinet Office. (1998) Data Protection Act 1998. London. HMSO

Cabinet Office. (1998) Human Rights Act 1998. London. HMSO

Cabinet Office. (1998) Crime and Disorder Act 1998. London. HMSO

Cabinet Office. (1990) Computer Misuse Act 1990. London. HMSO

Cabinet Office. (2000) Regulation of Investigatory Powers Act 2000. London. HMSO

Cabinet Office. (2000) Electronic Communications Act 2000. London. HMSO

Cabinet Office. (2000) Freedom of Information Act 2000. London. HMSO

Cabinet Office. (1990) Access to Health Records Act 1990. London. HMSO

Cabinet Office (1988) Copyright, designs and patents Act 1988. (as amended by the Copyright computer programs regulations 1992). London . HMSO

Cabinet Office (1998) Crime and Disorder Act 1998. London. HMSO

Cabinet Office. (2004) Children's Act 2004. London. HMSO

DOCUMENT PROFILE	
REFERENCE NUMBER	B0413
CATEGORY	Non-Clinical
VERSION	V5
DIVISION	Owning Division – Corporate
SPECIALTY	Owning Specialty – Information Governance
QUALITY ASSURANCE GROUP	IGHR Committee
AUTHOR	Thelma Turner Information Governance and Health Records Manager
ISSUE DATE	February 2018
REVIEW DATE	February 2021
OTHER APPROVING GROUPS	IGHR Operational Group (reviewed as sub group of IGHR committee
APPROVAL AND RATIFICATION DETAILS / DATES	Policy Approval: IHGR Committee – 29th September 2016, followed by E-Approval 27th February 2018 TPAG Ratification: 26th February 2018
EQUALITY IMPACT ASSESSMENT	B0413 RD2
CONSULTEES	Members of the Trust IGHR Committee and IGHR Specialist Group
DISSEMINATION DETAILS	Upload to Policy Site; cascade via IGHR Operational Group, IGT standard leads and divisions
KEYWORDS	Information Governance, Data Protection, Freedom of Information, IG Toolkit,
RELATED TRUST DOCUMENTS	Gloucestershire Information Sharing Partnership Agreement (GISPA) Clinical and Non-Clinical Information Systems Management Policy Intellectual Property Policy Internet and E-Communications Policy IT Security Policy Data Quality Policy Fax Protocol Action Card Records Management Policy (including requests for access through DPA and FOI) Link to the NHS Digital - Registration Authority Policy IG Forensic Readiness Guideline Portable IT Equipment and Removable Media Protocol Maternity Health Records Policy Storing and Sharing Electronic and Paper Records Research Governance
OTHER RELEVANT DOCUMENTS	Incidents - Managing, Reporting and Reviewing of Incidents / Accidents, including Serious Incidents CCTV: Usage and Code of Practice Contractors Disciplinary Procedure Mandatory Training Risk Management Strategy Risk Assessment / Risk Register Process Media, Celebrity and VIP Visitors Web Publishing Policy
EXTERNAL COMPLIANCE STANDARDS AND/OR LEGISLATION	• NHS Department for Health IG Toolkit • The Data Protection Act 1998. • General Data Protection Regulation (GDPR) • See also section 3 of policy for fuller list