# Information Governance Policy

| Version | Description of Change(s) | Reason for Change | Author | Date |
|---|---|---|---|---|
| 1.0 | | | | |
| 1.1 | Amendments made | Policy updates | C Sadler | 02/04/2014 |
| 1.2 | Review | Policy updates | C Sadler | 03/11/2015 |
| 1.3 | Review | Annual Review | ENW | 20/12/2016 |
| 1.4 | Review | Annual Review | R Meaker | 23/08/2017 |
| 1.5 | Amendments made | Policy Updates | R Bada | 08/10/2018 |
| 2.0 | Approved | | DSPG | 26/10/2018 |

## Policy Reference Information

| | |
|---|---|
| **Policy Reference Number** | **DSP 014** |
| **Version Number** | **1.5** |
| **Status** | **Approved** |
| **Author/Lead** | **Rob Meaker (Executive Lead)** |
| **Implementation Date** | **September 2013** |
| **Date of Last Review Date** | **23/08/2017** |
| **Date of Next Formal Review** | **August 2018** |
| **Ratified by** | **Audit and Governance Committee** |
| **Date of Ratification** | **8 January 2018** |
| **Date of Equality Impact Assessment** | **September 2013** |

## Contents

## 1. Introduction

Information governance is defined as the structures, policies, procedures and best practices that will be applied at all times by the Barking and Dagenham, Havering and Redbridge Clinical Commissioning Group (BHR CCGs), its employees, partner organisations and suppliers to ensure that confidentiality, security and appropriate handling of all records and information regardless of the format in which they may be held, to ensure ethical use in the best interests of patient care and the public good.

This policy sets out the principles to be adopted by BHR CCGs regarding the implementation of a governance framework for all information related activities; this governance framework will be known as 'Information Governance'. The organisation recognises that:

- patients are at the heart of everything the NHS does
- the focus should continuously be on improving those things that really matter to patients and the outcome of their healthcare
- Empower and liberate clinicians to innovate, with the freedom to focus on improving healthcare services

## 2. Purpose and Scope

Information is a valuable asset that must be protected at all times in both clinical delivery and the efficient management of services and resources. Information plays a fundamental role in supporting clinical governance, performance and service management.

It is therefore of high importance that information is effectively managed and that appropriate policies, procedures and management accountability structures are in place to provide a robust framework to deal with the many different information requirements including

- Information governance management
- Clinical information assurance
- Confidentiality and data protection
- Information security assurance
- Secondary uses assurance.

The aims of this document are to maximise the value of organisational assets by ensuring that data is:

- Held securely and confidentially
- Obtained fairly and lawfully
- Recorded accurately and reliably
- Used effectively
- Shared and disclosed appropriately and lawfully

So as to protect BHR CCGs information assets from all threats, whether internal or external, deliberate or accidental the organisation will ensure:

- Information will be protected from unauthorised access

- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested
- Information security training will be available to all staff
- All breaches of information security, actual or suspected, will be reported via the organisations'' risk and incident reporting processes and reviewed by the Data Security and Protection Group (DSPG). The Senior Information Risk Owner (SIRO) or group may require further investigation and request mitigations and improvement plans.

BHR CCGs' joint committee of governing ~~body~~ bodies acknowledges the importance of robust information governance and is fully committed to the development and maintenance of best practice in all areas of information management, thereby minimising the risk to the organisations', its service users, staff and contractors.

The organisation recognises that timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes.

The organisation acknowledges the necessity to share patient information with other health organisations, approved partners and other agencies in a controlled manner consistent with the interests of the patient and, in certain circumstances, the patient's or public interest.

The governing body undertakes to put into place an appropriate structure, and commit the necessary resources to ensure an appropriate programme of work is initiated and sustained for this purpose. The DSPG will undertake, on behalf of the Audit and Governance Committee a monitoring role to oversee the process against targets set out within the Data Protection and Security Toolkit.

## 3. Background

Information Governance is the information component of Clinical Governance and Corporate Governance and brings together in a single framework legislation, requirements and standards including

- The Data Protection Act (DPA) 2018
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice
- The NHS Care Record Guarantee (for England)
- The Social Care Record Guarantee (For England)
- The international Information Security Standard ISO/IEC 27001:2005
- The Information Security NHS Code of Practice
- The Records Management Code of Practice
- The Freedom of Information Act 2000

This policy applies to all information systems that, at any time, may be deployed, purchased, developed or managed by/or on behalf of the organisation and any individual directly employed or otherwise engaged by the organisation.

It covers all aspects of processing activities (any activity performed when handling information i.e. collecting, storing, handling, sharing or disclosing etc.), that relate to (but is not limited to):

- Patient/Client/Service User information
- Personnel/Staff related information
- Corporate information

And covers all formats/modes of information processing, including (but not limited to):

Structured and unstructured record systems - both paper and electronic ‘

- Transmitted information – fax, e-mail, post and telephone.

The policy is underpinned by and must be read in conjunction with the specific Information Governance policies and procedures that support the effective implementation of the information governance framework. A list of the relevant key policies is provided in Appendix B.

## 4. Benefits

Implementation of this policy and all other associated policies will contribute towards providing assurances to the organisations’ stakeholders, (i.e. patients, approved partners, staff) that their information has been processed in accordance with legislative, ethical and national NHS policy requirements and DPA principles.

Implementation of the policy and an effective information governance framework will support risk mitigation and reduce the risk of governance breaches. Serious governance breaches can lead to prosecution under the DPA Act (2018) or an action for civil damages which could result in costs, and a loss of reputation and patient trust; the Information Commissioners Office (ICO) can also impose fines of up to 20 million Euros (or equivalent in sterling) or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

## 5. Principles

The following shall be applied by the organisation’s to ensure that Information Governance related activities include the following:

- The organisation recognises the need for an appropriate balance between openness and confidentiality in its processing of information.
- The confidentiality of personal identifiable information is paramount and will be guided by the requirements set out within Confidentiality - NHS Code of Practice Parts 1 and 2, and other legislative requirements.
- Patients have the right to access information relating to their own health care, held within health records. All Staff members have the right to be provided with access to their employment records. There are clear procedures and arrangements for the handling of queries known as Subject Access Requests (SARs).
- For further information;

Staff Subject Access Request

Patient Subject Access Request

- Identifiable patient data shall only be accessed for handling complaints, dealing with continuing healthcare cases, processing individual funding requests or for work carried out by the Medicines Management Team. Any exceptions to this rule, i.e., any intended use of identifiable patient data accessed for other purposes is;
    - Authorised only upon receiving explicit written consent from the patient involved. In the process you must obtain written consent for all future intended use of the information. If the patient objects to any aspect of the request, these wishes must be respected. Additional uses cannot be added without the patient's consent. The patient has the right to withdraw consent at any time.
    - Exemptions as identified in the Data Protection Act (2018)
- In necessary circumstance the organisation will always use pseudonymised or anonymised data as opposed to person identifiable information.
- All personal identifiable information relating to staff is also considered as confidential information.
- Due diligence should always be taken when handling information of a confidential and sensitive nature.
- There will be an on-going training and awareness raising campaign for all staff, clearly defining their specific responsibilities to ensure that the confidentiality or security of personal identifiable information is not compromised.
- Contracts or Service Level Agreements for any third party individuals or companies required to carry out work for, or on behalf of the organisation (irrespective of whether they are expected to have access to personal information or not), must contain information governance basic principles (do's and don'ts) and relevant confidentiality clauses that must be signed prior to any placement commencing.
- Information that is not considered to be confidential in nature (i.e. not of a sensitive nature, person identifiable or commercially sensitive corporate information) will be made available to the public in line with the Freedom of Information Act 2000 via the organisation publication scheme. The organisation will establish clear procedures for staff to follow to ensure that all received Freedom of Information requests are recognised and handled in both an appropriate and legal manner.
- NEL CSU manages on behalf of the organisations' all FOI requests and Environmental Information Regulations 2004 (EIR) requests received.
- The organisation will process all requests concerning information in relation to the environment (e.g. Air Quality, Road network infrastructure etc.) under the terms of the Environmental Information Regulations 2004.
- The organisations will establish and maintain policies and procedures for the effective and secure management of its information assets and resources, these will include Information Security, Data Protection/Confidentiality, Corporate Governance (including Freedom of Information) and Information Lifecycle/Data Quality/Records Management Policies.
- Audits will be undertaken or commissioned to assess information and Information Communication Technology (ICT) security arrangements.
- The organisations risk management strategy will be utilised to minimise and mitigate risks with regards to information processing activities. Corporate and local risk and incident management and reporting procedures must be implemented.

- From June 2013 all organisations processing health and social care personal data are required to use the IG Toolkit Incident Reporting Tool (now replaced by the Data Security and Protection reporting tool) to report level 4 IG Serious Incidents Requiring Investigation (SIRI) to the NHS Ddigital DSPT, NHS England and Information Commissioner's Office.
- The organisation will establish and maintain policies and procedures for the effective management of records and Information Quality Assurance in line with the Department of Health Records Management Code of Practice, Parts 1 and 2.
- Improvements in the integrity of information processes are to be promoted, monitored and sustained. The organisation will promote and encourage these improvements through training, policy development and other awareness raising initiatives.
- Audits will be undertaken to ensure the quality of data and records management activities. Wherever possible, information quality will be assured at the point of collection.

## 6. Accountabilities and Responsibilities

### 6.1 The Governing Body (GB)

The organisation will define the strategy and policy in respect of Information Governance, taking into account the associated legal and other frameworks, including: The Data Protection Act (2018), Freedom of Information Act 2000, The Common Law Duty of Confidentiality, The Public Records Act 1958 and any other relevant legislation and direct/indirect NHS requirements. The GB is responsible for ensuring that sufficient resources are provided to support the requirements of the strategy and supporting policies.

### 6.2 Accountable Officer (AO)

The Accountable Officer is accountable for ensuring that the organisations complies with its statutory obligations and has overall accountability and responsibility for Information Governance. The Chief Officer is required to provide assurance, through the Statement of Internal Control and other methods (e.g. DSPT), that all risks, including those relating to information, are effectively managed and mitigated.

### 6.3 Data Protection Officer (DPO)

The DPO assists in monitoring internal compliance, inform and advice on the ~~CCG's~~ CCGs' data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact for data subjects and the supervisory authority. The DPO will report directly to the highest level of management and is given the required independence to perform their tasks. The DPO must perform the tasks as defined in article 39 of the General Data Protection Regulation/Data Protection Act 2018.

### 6.4 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) for the organisation is responsible for ensuring that the Information Risk Policy is developed, implemented, reviewed and its effectiveness frequently monitored. The SIRO provides the focus for the assessment and management of information risk at Board level providing briefings and reports on matters of performance, assurance and cultural impact with regards to Information Risk.

The SIRO will be an Executive Director or other senior member of the Board (or equivalent senior management group/committee) but cannot also be the Caldicott Guardian.

The SIRO will understand how the strategic business goals of the organisations may be impacted by information risks. The SIRO will act as an advocate for information risk on the GB and during internal discussions, and will provide advice on the content of the annual Statement of Internal Control (SIC) in regard to information risk.

Other key responsibilities of the SIRO are to:

- take ownership of the assessment process for information risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control
- ensure that BHR CCGs approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- provide a focal point for the resolution and/or discussion of information risk issues and review and agree action/s needed in respect of mitigating identified information risks
- Ensure that the GB is adequately briefed on all potential and actual information risk issues.

**6.5 Caldicott Guardian**

The Caldicott Guardian should be, in order of priority:

- an existing member of the senior management team;
- a senior health or social care professional (with clinical expertise); and/or
- The person with responsibility for promoting clinical governance or equivalent functions.

The Caldicott Guardian plays a key role in ensuring that the NHS and all other partner organisations satisfy the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of an organisation, the Caldicott Guardian supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. The Caldicott Guardian will also play a strategic role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level.

**6.6 Information Asset Owners (IAO) and Information Asset Administrators (IAA)**

Information Asset Owners (IAO's) are Directors or Senior Managers accountable for the identification and management of their Information Assets, Information Flows and Information Risk management within their directorate. The IAO's role is to understand and address risks to the information assets they 'own'. The IAO is accountable to the SIRO and will and provide assurance on the security and use of their assets and that information risk is effectively managed.

IAOs are responsible for ensuring the effective Implementation of information governance policies and procedures. They must make sure that staff are kept up to date with any changes to working practices in line with policies and procedures in relation to Information Governance, and address any identified areas of non-compliance.

IAO's must ensure they have adequate knowledge of what information is held within their directorate along with a detailed understanding of the information flows to and from all of the assets for which they are responsible. Routine flows of patient data should be assessed periodically and justification of that flow maintained at all times.

IAO's may appoint Information Asset Administrators (IAA) to provide operational support (to the IAO). The IAA will be responsible for monitoring compliance with policy, identifying and reporting all encountered risks and incidents, and ensuring that the information asset register is updated accurately to reflect any changes to said assets. The IAA will undertake day to day responsibility for management of assets reporting back to the IAO as necessary.

### 6.7 Information Governance Leads (Executive)

The Information Governance Lead will be responsible for:

- Ensuring that information governance issues remain as a key priority at GB level;
- Development and maintenance of documentation that demonstrates commitment to and ownership of information governance (IG) responsibilities;
- Ensuring that there is sufficient, top level awareness and support for IG resourcing and implementation of improvements throughout the organisation;
- To co-ordinate the collation of evidence for the DSPT Toolkit;
- Providing direction in developing and promoting all IG related policies;
- To co-ordinate the activities of staff given IG responsibilities and progress initiatives;
- Ensuring annual assessments and audits of IG policies and arrangements are carried out as required and all findings reported;
- Ensuring that the approach to patient confidentiality and the secure handling of all confidential information is communicated clearly to all staff;
- To identify, facilitate and monitor different levels of IG training that should be made available throughout the organisation to all staff, determined by the specific requirements of their job role;
- Liaising with other committees, steering groups and programme boards, as is required in order to promote and integrate IG standards;
- Monitoring information handling activities to ensure compliance with the law and guidance;
- To be a support mechanism, providing a focal point for the resolution and/or discussion of all encountered IG issues;

### 6.8 Management Staff

Directors, managers, staff with managerial or supervisory designated responsibilities are accountable for ensuring that good information governance practices are embedded within their areas of their control. This includes but is not limited to:

- Ensuring that national and locally agreed Information Governance standards are upheld within their department
- Maintaining awareness levels for all staff, in relation to their specific responsibilities for information security, data protection and confidentiality and quality of data
- Determining and monitoring required access levels to specific computer systems ensuring that no unauthorised access of any systems, is at any time occurring
- Ensuring that adequate training is provided to all staff
- Ensuring that all staff fulfil their obligations by completing all identified training.
- Implementing procedures to minimise risk e.g. human error / risk of fraud / theft / disruption of their systems
- Ensure documentation is maintained and periodically reviewed for all critical job functions
- Supporting planned evaluations of Information Governance and any resulting actions
- Investigating any information governance issues that may be raised / identified by members of the public, patients, visitors or staff e.g. Complaints, Risk Management. Reporting all findings in an open manner and escalating more serious issues as is deemed necessary.

### 6.9 Individual Responsibilities

All staff will be responsible for effective information governance including (but not limited to):

- Discharging of their legal, ethical and contractual responsibilities for processing information regardless of their position (whether directly employed or not), standing or level of knowledge. This includes permanent, temporary, locums, voluntary, work experience and bank staff, including contractors and partners involved in the organisation business related activities
- Abiding by legislations, professional standards, codes of conduct, policies and any locally agreed standards
- To report immediately any actual or potential threats that may be encountered in relation to Information Governance /Security
- To ensure full compliance to this policy and all other Information Governance related documentation that may be issued throughout the organisations'.
- To ensure that any relevant, mandatory Information Governance training is completed annually. Staff who has taken on additional responsibilities must ensure that they complete any additional relevant IG training in order to equip them with the skills and knowledge to perform their duties to a continual high standard.
- At all times to strive to achieve best practice standards with full compliance towards professional codes of conduct. For further information please visit:

  www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/lglobligat.pdf

## 7. Risk Management

The organisations' Risk Management Framework will inform the process for the control of Information Governance related risks, however:

- All staff, whether substantive, temporary or on a voluntary basis etc., must be aware of and comply with this and all other Information Governance related policies and procedures.
- Staff must be made aware of the implications and the consequences of non-compliance e.g. where confidentiality may be breached. These should be clearly disseminated to all concerned and assurance of understanding of the potential disciplinary and legal implication that may be incurred if found to be in breach.
- All breaches whether actual or suspected, including near miss incidents that may have placed the availability, confidentiality or integrity of information at risk must be reported. Reporting of incidents does not replace the right of persons who may have genuine concerns from pursuing the matter via the organisations' Whistle Blowing Policy.
- Failure to observe and abide by said policies, procedures and processes may be regarded by the organisations as gross misconduct. Individuals involved in BHR CCGs activities must be made aware that disciplinary procedures, civil action or criminal proceedings may be instigated as a consequence of damage caused to an individual or organisation.
- The Information Governance Steering Group will monitor IG related risks, incidents and breaches and may request action plans, details of mitigating actions and any lessons learnt. The IG Lead may request or undertake a formal investigation.

## 8. Training and Awareness Raising

The SIRO has the overall responsibility for ensuring that all staff are made aware of the requirements of the DPA / GDPR and their IG obligations and this will be carried out by regular mandatory Information Governance training sessions. Any new staff members (including temporary, contractors) will be required to complete Information Governance as part of their induction.

Information Governance training is required to be undertaken by all CCGs employees and those providing a service to the CCGs. All NHS staff are mandated to undertake annual Information Governance training.

Where staff have specific Information Governance roles within the CCG i.e. Caldicott Guardian, SIRO etc. additional Information Governance training will be required. Additional training will be made available to all persons, where it is required. For further guidance refer to the Information Governance Training Needs and Analysis (TNA) document.

To maintain high staff awareness the CCG will direct staff to a number of sources:

- Policy/strategy and procedure;
- Manuals;
- line manager;
- specific training courses;

- other communication methods, for example, team meetings; and staff Intranet. See Appendix D for additional information

## 9. Audit monitoring and Review

Monitoring of the information governance framework will be managed through assessment by and compliance with the requirements as set out within the NHS Digital's DSPT. The DSPT assessment will also provide the basis for on-going planning.

The organisation must demonstrate compliance by completing each mandatory assertion on the DSPT and be submitted by the end of March 2019.

Identified leads for each of the initiatives will be responsible for establishing and providing verifiable evidence for the attainment scores.

The process for the annual Information Governance Baseline Assessment will be advised and overseen by the Data Security and Protection Group and:

- An annual compliance report, together with regular improvement plans detailing identified targets for improvements shall be submitted to the Joint Management Team, and if necessary escalated to the Data Security and Protection Group.

This policy will be monitored and will be subject to 24 month regular review however an earlier review may be warranted and will be carried out without prior notification should one or more of the following occurs:

- As a result of regulatory / statutory changes or developments;
- As a result of NHS policy changes or developments; or
- For any other relevant or compelling reason as is deemed necessary.

## 10. References

- Data Protection and Security Toolkit:
  https://www.dsptoolkit.nhs.uk/
- Information Governance Training Tool:
  https://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm

  https://bhrccgs.nhsworkforce.org/applications/elearning/course/book/
- Data Protection Act 2018:
  http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Freedom of Information Act 2000:
  www.informationcommissioner.gov.uk/
- Human Rights Act 1998:
  http://www.justice.gov.uk/human-rights
- Processing and Using Patient Information – A Manual for Caldicott Guardians:
  http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/caldresources/guidance
- Environmental Information Regulations 2004 -
  http://www.ico.org.uk/for_organisations/environmental_information/guide/act

- Confidentiality – The NHS Code of Practice:
  https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- NHS Commissioning Board Information Governance Policy
  http://www.england.nhs.uk/wp-content/uploads/2012/11/info-gov-pol.pdf
- NHS Care Record Guarantee
  http://www.nigb.nhs.uk/pubs/nhscrg.pdf
- ISO/IEC 2700:2005
  http://www.iso.org/iso/home/standards.htm
- The Records Management Code of Practice
  https://www.gov.uk/government/publications/records-management-nhs-code-of-practice.

## 11. Appendix A

### Glossary

| Term | Definition |
|---|---|
| DoH | Department of Health |
| DPA | Data Protection Act |
| DSPG | Data Security and Protection Group |
| DSPT | Data Security and Protection Toolkit |
| FoI | Freedom Of Information |
| GDPR | General Data Protection Regulation |
| HSCIC | Health and Social Care Information Centre |
| IAA | Information Asset Administrator |
| IAO | Information Asset Owner |
| ICO | Information Commissioners Office |
| IG | Information Governance |
| IGT | Information Governance Toolkit |
| organisation | Barking and Dagenham, Havering and Redbridge Clinical Commissioning Groups (BHR CCGs) |
| PID | Person/Patient Identifiable Data |
| SIC | Statement of Internal Control |
| SIRI | Serious Incidents Requiring Investigation |
| SIRO | Senior Information Risk Owner |
| SLA | Service Level Agreement |
| TNA | Training Needs Assessment |

## 12. Appendix B
## RELATED ORGANISATION KEY INFORMATION GOVERNANCE POLICIES/ PROCEDURES

- Information Governance Management Framework
- Information Security and Access Control Policy
- Data Protection and Confidentiality Policy
- Corporate Governance (including FOI)
- Information Lifecycle Management Policy (including Records Management and Information Quality)

## 13. Appendix C
## 14. RELEVANT LEGISLATION / GUIDANCE

This section is a summary of key legislation and NHS Guidance relating to Information Governance.

**Data Protection Act 2018**

The purpose of the Act is to safeguard the fundamental rights of individuals and to protect them with regard to processing personal data about them. The Act is regulated by the ICO and contains 6 main principles governing the processing of personal data:

**Principle 1: Lawfulness, fairness and transparency**
To remain lawful, the organisation needs to have a thorough understanding of the GDPR and its rules for data collection. To remain transparent with data subjects, the organisation should state in our privacy policy the type of data we collect and the reasons for collecting it.

**Principle 2: Purpose limitation**

The organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.

**Principle 3: Data minimisation**
Organisations must only process the personal data that they need to achieve its processing purposes.

**Principle 4: Accuracy**
The accuracy of personal data is integral to data protection. The GDPR states that "every reasonable step must be taken" to erase or rectify data that is inaccurate or incomplete.

**Principle 5: Storage limitation**
The organisation need to delete personal data when it's no longer necessary.

**Principle 6: Integrity and confidentiality**

Personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"

The Act imposes strict regulations and it is important that these standards are adhered to at all times. Staff must be fully aware of how patient information is processed across the organisation, and of the procedures for providing access to information in order to respond to patient enquiries. Further information on Data Protection can be found in the organisations Information Security Policy.

**The Caldicott Principles –** In 1997 Dame Fiona Caldicott carried out a review of Information Sharing within the NHS. This review led to the introduction of 6 Principles which would need to be considered by anyone handling patient data so that prior to sharing they should always consider beforehand in order to justify the sharing of that data. They are as follows:

1. Justify the purpose(s) of using confidential information

2. Only use it when absolutely necessary

3. If you have to share person identifiable information, use only the minimum that is required

4. Access should be on a strict need-to-know basis (are they involved in delivering healthcare to that patient if not they are not authorised)

5. Everyone must understand his or her responsibilities

6. At all times to understand and comply with the law

Following a request from the Secretary of State for Health, Dame Fiona Caldicott was asked again to carry another independent review of information sharing in 2012 with a report published during April 2013 in order to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care within the NHS. Following the completion and findings of the review, there has been the proposal put forward for the implementation of a seventh principle;

7. The duty to share information is as important as the duty to protect

The Caldicott Guardian should always be consulted for support/guidance in association with information sharing / disclosure scenarios.

**Access to Health Records Act 1990**

Under the Data Protection Act 2018 individuals (patients and staff) have the fundamental right to have access to personal records held about them. Access to medical records was previously covered by the Access to Health Records Act 1990, but this Act now only covers any requests made for access to health records relating to deceased patients. All others requests are dealt with under the requirements of the Data Protection Act.

**Freedom of Information Act 2000**

The Freedom of Information Act came into fully into force in January 2005 and creates a statutory right for an individual to know whether a public authority holds specified corporate information, and, if it does, to have that information communicated. Whereas the Data Protection Act 2018 deals with the rights of individuals regarding their own personal information, the Freedom of Information Act covers corporate information. The Act also requires public authorities to release information, as a matter of routine, pro-actively through an approved publication schemes. In order for the authority to locate the information requests from individuals must be clear and in writing. The organisation has a responsibility to respond to requests within 20 working days of the request being received. The Act, like the DPA 2018 is regulated by the ICO. There are some exemptions to the Act, including personal information that is covered by the Data Protection Act.

**The Common Law Duty of Confidentiality**

Common Law is the law of precedent. It is not written down anywhere and relies up on the application of the findings in previous Court cases as decided by judges.

The Common Law Duty of Confidentiality means that it has previously been established that when there is an 'expectation' of confidentiality between two parties (e.g. between a Healthcare Professional and a Patient), that confidence will be respected and not be broken without the explicit consent of the patient.

In practice all information that may be held concerning a patient, regardless of whether it may be held on paper, in an electronic file on a computer, a video or audio tape, or even if this information is simply held within the memory of a Health Professional, it must not be disclosed or divulged to a third party without the consent of the patient.

It is irrelevant whether the patient is old, has mental health issues or is deemed to lack mental capacity. The duty of confidentiality still applies.

There are however four sets of circumstances in which the disclosure of confidential information to a third party is lawful**:**

- where the patient has given consent
- where disclosure is in the overriding public interest
- where there is a legal duty to disclose for example by court order
- where there is a statutory basis which permits disclosure

It is clear that disclosure of patient identifiable information is restricted by the **Duty of Confidentiality under Common Law** to those Health Professionals providing care to the patient.

**Health Professionals** are usually aware of their duty of confidentiality in relation to one-to-one consultations and in relation to written health records or consultations; curtains are not sound proof and other patients or staff may be likely to overhear. Health Professionals must take care not to discuss patient related matters in public places, such as the staff car park or restaurant.

The **Caldicott Guardian** has a responsibility to ensure that all staff are aware of the need to comply with the **Common Law Duty of Confidentiality** at all times and not just in relation to formal records. On the other hand there will be circumstances where information relating to patients should and can be released without breaching these principles. It is acceptable to include patient data which has been anonymised or depersonalised to support research work or to answer requests for information - the concept of confidentiality of patient identifiable data should not be confused with the use and application of patient data which is not individually identifiable.

**Staff Awareness** – staff involved in any stage of sharing and disclosing data and information must fully understand and comply with this policy and all other relevant policies. Staff must understand that they may be liable for any such loss, and that any breaches of this or any other policy may result in disciplinary action including dismissal. Staff must also be aware that they may be held personally liable by the Information Commissioner. If found in breach; the organisation could be subject to a fine of up to 20 million Euros or 4 percent of annual global turnover, whichever of both is highest.

**Third-party Awareness** – any user or third-party sharing and disclosing data and information on behalf of the organisations must comply with this policy and all other relevant policies. Where third-parties do not comply with this Policy or any other relevant policy, the organisations will reserve the right to terminate all current contractual agreements with immediate effect and without prior notification. Third-party providers and their staff must also be aware that they may be held personally liable for any non-compliance with their statutory

requirements by the Information Commissioner and could face substantially large fines. As a matter of routine the ICO now publishes all monetary fines issued via their website.

## 15. Appendix D – Training

This tool allows users to learn about essential IG topics and test their knowledge and understanding. It also stores your training progress as you go through the e-learning training.

The organisation must be able to demonstrate completion of IG Training for 95% of staff members for each and every financial year. The target staff groups listed below are required to ensure that they attend this programme.

Details of the modules for completion are as follows:

- All Staff must complete the Information Governance module on the CSU Workforce
- SIRO – '*NHS Information Risk Management module for SIRO's and IAO's'*
- Caldicott Guardian – '*The Role of the Caldicott Guardian in the NHS and Social Care'*
- IAOs / IAA's – *'NHS Information Risk Management module'*
- Staff with daily exposure to patient identifiable data who may be asked for patient information during the course of their duties - *Access to information and information sharing in the NHS*
- Staff with Records Management responsibilities – Dependent on level of responsibility allocated, it will be a combination of the following modules :
    - Records Management & the NHS Code of Practice
    - NHS Information Risk Management

**This list is the current minimum there may be additional training identified for completion by staff with key IG responsibilities without prior notification.**

## 16. Appendix E

### Equality Impact Assessment Tool

**Equality Impact Assessment Form - Policy**

| Equality Impact Assessment Form | | |
|---|---|---|
| Policy author: Rob Meaker | Date of assessment: September 2018 | |
| Title of policy: Information Governance Policy | Is this a new or existing policy? EXISTING | |
| 1. Is there a concern that the policy does or could have a differential impact in any of the following areas? | | |
| | Y/N – delete as appropriate | |
| Age | Yes | No **X** |
| Civil partnership/marriage | Yes | No **X** |
| Disability | Yes | No **X** |
| Faith or religious beliefs | Yes | No **X** |
| Gender | Yes | No **X** |
| Race | Yes | No **X** |
| Pregnancy/maternity | Yes | No **X** |
| Sexual orientation | Yes | No **X** |
| Transgender | Yes | No **X** |
| 2. If the answer is 'no' for the groups above, please sign and date the form and add this form to the end of the policy.<br>3. If the answer is 'yes' for any of the groups above, please explain the reasons and complete box 4 (below). For help please contact the engagement adviser for advice (020 8926 5048). | | |
| 4. Are there any additions or actions to be added to the policy which ensure the policy does not have an adverse impact on any of the protected groups? If the answer is "yes", please detail below. | | |
| **Signed:**<br>(Policy author) Rob Meaker | **Date:** September 2018 | |
| Your contact details<br>(department; e-mail; telephone number) | **rob.meaker@nhs.net** | |