NHS
Bristol Clinical Commissioning Group

# Information Governance Strategy

# Includes ‘Information risk’ & incident management methodology & education approach

**Approved by: Governing Body**

**Ratification date: March 2016**

**Review date: March 2017**

## Document Status

| **Information Governance Strategy** | |
|---|---|
| **Document Status** | Version 2.0 |
| **Document Author(s)** | Adam Tuckett |
| **Document Owner** | Chief Financial Officers & Caldicott Guardians |
| **Client** | Clinical Commissioning Groups |
| **File Reference** | |
| **Date Issued** | February 2014 |
| **Approved by and date of approval** | |

## Revision History

| **Avon IM&T Consortium** | | |
|---|---|---|
| **Document status: current** | | |
| **Version** | Date | Comments |
| **1.0** | 17th December 2004 | First draft for comment & PCT specific tailoring |
| **1.1** | 28th January 2005 | Minor amendments following team comment |
| **1.2** | 04 May 2005 | Made current following PCT board approvals – included one amendment relating to scope including support for independent contractors. |
| **1.3** | January 2006 | Minor update in line with revised Information Governance Policy and to reflect up coming PCT structure changes. |
| **1.4** | October 2008 | Review and update to reflect organisational and sector developments, particularly the role of Senior Information Risk Owner |
| **1.5** | November 2010 | Review and update to reflect changes in IG toolkit and to set out as suitable for future planned organisational structures – no fundamental changes, but improved throughout |
| **1.6** | Jan 2012 | Reference BNSSG Cluster and Information Risk Group |
| **1.7** | Jan 2013 | Prepared and altered for Clinical Commissioning Groups |
| **1.8** | June 2013 | Amended to reflect changes to incident reporting via IG toolkit. |
| **2.0** | February 2014 | Annual update – including Caldicott 2 recommendations |
| **3.0** | January 2015 | Review in relation to Audits of IG toolkit v12 |
| **4.0** | March 2015 | Review in relation to Audits of IG Toolkit v13 |

## Contents

## 1 Purpose

The organisation is required to have effective arrangements in place to govern the uses of information and information systems in the organisation. This strategy sets out the scope and approach that the organisation will operate to ensure legal and regulatory compliance and where practical best practice in handling information is achieved.

## 2 Background

Information Governance has developed as a programme of work to encompass all aspects of handling information and compliance with legislation including Data Protection Act (1998) and the Freedom of Information Act (2000), and meeting regulatory standards for records management, information security and data quality. It recognises the significant overlap in activities, knowledge and skills required for these areas and aims to ensure consistency and efficiency of approach to deal with related matters.

The Department of Health have set standards and a measure of compliance within the 'Information Governance' toolkit. Performance of organisations relates to a number of core standards set by the Care Quality Commission.

In the wider context organisations are now subject to significant monetary penalties if they are found to have failed in their responsibilities under the Data Protection Act 1998. Numerous large fines have been imposed by the Office of the Information Commissioner. As a result organisations are required to report any Serious Incidents Requiring Investigation (SIRI) and provide assurance of compliance with information governance standards in the annual report.

In 2013, the Information Governance Review 'To share or not to share' (Caldicott 2) was published. This strategy has been revised in light of the recommendations accepted by the Government response.

It is also recognised that effective governance of information is a key supporting element to making best use and gaining real benefit from the information resources.

## 3 Scope

Information Governance is an 'umbrella' term for a number of linked initiatives which are categorised in the Information Governance toolkit as follows:

- Confidentiality & Data Protection – staff responsibilities and patients' rights
- Corporate information – Freedom of information and records management
- Clinical information – Health records management
- Information Governance Management – operational framework
- Secondary Uses of information – appropriateness and quality
- Information Security – technical and organisational security processes

The scope is clearly wide with some impact on every member of staff. For an organisation to ensure an appropriate level of compliance, many individuals and groups across the organisation are required to have specified responsibilities. The groups and staff are identified later and responsibilities are detailed in the Information Governance Policy. The scope of this strategy is to set out the structure for Information Governance Management and activity, ensuring that the organisation addresses all areas effectively.

## 4 Strategic approach & objectives/deliverables

The fundamental objective for the strategy is to promote positive compliance with legislation and standards and by consequence reduce risk, with risk being identified in a number of categories:

- Loss of public trust/confidence in the organisation (due in particular to losses/inappropriate disclosures)
- Contribution to, or cause of, clinical or corporate negligence (due to unavailable, inaccurate, incomplete or out of date information)
- Legal action including fines, for non compliance with Data Protection, Common Law, Human Rights and Freedom of Information legislation

So in assessing activities to comply, the Information Governance lead and other staff will evaluate requirements from a risk management perspective, utilising where possible existing risk assessment methods (CRAMM) and standards (ISO27000 series).

A ‘whole systems’ approach is fundamental to an effective Information Governance framework. To this extent the work of the Information Governance team will incorporate the following core work streams, directed towards ensuring implementation of the IG policy and requirements of compliance with the IG toolkit:

- **Information Governance Management System** – ensuring that the approaches and methods for handling information are clearly documented and evidenced. This will include oversight of information governance work by appropriate committee.
    - **Deliverables -** a robust framework of policy and guidance that is approved owned and promoted by the organisation. Incorporating workplans to maintain and improve compliance.
- **Education and awareness programme** – of staff, partners, contractors and patients, achieved via formal and informal education and awareness programmes and a process to review and ensure compliance for all new uses of information both in terms of information systems and development of healthcare services. This stream is guided by the IG Education Strategy and Data Protection Communications strategy (No Surprises – informing patients)
    - **Deliverables –** A programme of educational activities that provide core education to all staff, which assesses staff knowledge and provides further support as required. Additional educational activities delivered to the staff that need them. Via periodic organisation wide training needs analysis.
- **Technical security solutions** – establishing where technical solutions can aid the reduction of risk around handling data, but do not put unnecessary burdens on staff working practices. This is overseen by the Information Governance Group and managed on a day to day basis by an integrated programme between IG and IT services and linked to audits and risk assessment activities to identify requirements.
    - **Deliverables** – Any technical solution to improve security will be part of a defined business case (if needing funding) and project plan. Deliverables will be specifically defined within these.
- **Information risk assessment programme (including security)** – relating to compliance with policy and process and effectiveness of technical solutions and covering all aspects of related work, including system use, facilities, corporate records etc. This area includes specific local and internal audit programmes. This has a specific focus on knowing what information is held (information assets),

where it comes from and where it goes to (information flows) and managing times when it is unavailable (business continuity)

- **Deliverables** – regular risk reviews of systems, processes as part of the annual assurance and improvement work plan for information governance. Annual reviews of the security of key information assets and information flows will be undertaken to ensure security is achieved and maintained as far as possible. Confidentiality & system usage audits will also be undertaken.

There are also significant work programmes in other areas that support Information Governance compliance, namely:

- Date Quality work – linked to performance, contract monitoring and secondary uses of data extracted from the patient record. This also incorporates work to ensure that the use of Patient Confidential Data (PCD) is controlled appropriately within the framework of 'Accredited Safe Havens' and 'Controlled Environment for Finance (CEfF)'. (This service is provided by South Central & West Commissioning Support Unit to Bristol CCG).

An annual workplan for assurance and improvement will be established as part of the end of year IG toolkit compliance assessment - see section 6 for more detail.

**Compliance objectives:**

**April 2015 – March 2016**

- Consolidate compliance position and define further improvements and assurances required.
- Move activities to regular review, including information asset, data flow risk reviews stating the legitimate purpose for processing personal confidential data (PCD). Establish rolling programme of detailed risk assessments for key assets
- Establish compliance assurance programme of core processes and technical control measures (such as mobile working, system access control)
- Light touch review of 'how we handle your information' leaflet in progress

**April 16 onwards**

- Maintain strong, robust IG approach supporting requirements such as DSCRO, ASH, and CEfF
- Review of education and training programme including identification of specific educational needs and develop delivery programme

## 5 Accountability

**Accountable officer:** As required by the 'statement of internal controls' the accountable officer is the Chief Financial Officer.

Support is provided by the following roles:

**Senior Information Risk Owner (SIRO):** The role currently resides with the Chief Financial Officer and is required to be an executive board member. The role is to act as an advocate for 'information risks' and will provide the statement of internal control.

The role will lead the identification and management of information risks that will affect the strategic direction of the organisation as well as being responsible for the management of serious incidents. Whilst the role should have an overview of all areas of information governance as defined in section 3 (scope), it will pay particular regard to 'information security', 'information governance management' and 'corporate information assurance'.

**Caldicott Guardian:** The guardian should be ideally a board member and a registered clinical professional. The focus of the role remains the use of patient data and in terms of the work areas within information governance, the role will focus on confidentiality/data protection, clinical information and secondary uses of patient data.

**Information Governance Lead:** The IG Lead for the CSU is the Head of Information Governance. The Head of IG will operate the IG Framework, in order to maintain, check and improve the required areas of compliance. They also act as the Information Security Manager, in conjunction with key roles in IT Services

The table below illustrates the work areas, the key operational lead and the committees in place to oversee the required operational and development activities:

| **Assurance Area (from DOH IG toolkit)** | **Overseeing committee** | **CCG Lead staff/AIMTC support** |
|---|---|---|
| Confidentiality & Data Protection | Quality & Governance Committee | Caldicott Guardian / Information Governance Manager |
| Clinical Information | Quality & Governance Committee | Caldicott Guardian / Information Governance Manager |
| Information Governance Management | Quality & Governance Committee | SIRO Chief Financial Officer / Information Governance Manager |
| Secondary Uses | Quality & Governance Committee | SIRO Chief Financial Officer/ Information Governance Manager & Head of Business Intelligence CSU |
| Information Security | Quality & Governance Committee | SIRO Chief Financial Officer / Information Governance Manager & Head of IT – responsibilities as allocated in IT Services – IG responsibilities matrix |

**(please note, secondary uses is not part of the CCG version 11 IG toolkit, but expected to be included in due course)**

## 6 Management of workplan and compliance assessment

An information governance workplan will be developed and maintained. It will be monitored by regular reports to the Quality & Governance Committee. Reporting will enable the Quality &Governance Committee to:

- Monitor and direct activities to improve compliance with requirements
- To review and agree policies, processes and guidance
- To ensure operational support for queries, education, service development and audit/assurance is in place and effective.

The workplan will be managed by the Information Governance Manager (SWCSU). It will be overseen by the Senior Information Risk Owner and Caldicott Guardian.

Improvements will generally be measured by increase in scores within the IG toolkit, unless a specific goal is linked to a particular activity.

The programme will identify the resources required and responsibilities within the CCG and SWCSU to deliver the programme. It will also identify timescales by which activities are intended to be completed.

The SWCSU Information Governance team will undertake the annual assessment required by the IG toolkit and will submit the results within the time frame dictated by the Health & Social Care Information Centre (currently end of financial year). In addition any mandated ‘mid year’ assessments will also be undertaken

Improvement and update of the scoring will be undertaken throughout the year, so that the audit is not left until the last month or two of the financial year. Approval of the score to be submitted will be gathered from the SIRO and Caldicott Guardian and Quality & Governance Committee.

# 7 Relationship with the Commissioning Support Unit

The Commissioning Support Unit (CSU) will be undertaking a number of key activities on behalf of the CCG. The CCG will therefore require assurance from the CSU that the processing of personal data that it undertakes on behalf of the CCG is done in an appropriate and secure manner. The CSU is required to undertake regular assessment of compliance with information governance and improvement action where required.

Requirements on the CSU will be part of the Service Level Agreement (including an information sharing agreement) between the parties, which stipulates the CCG as the legal ‘data controller’ of personal data and that the CSU will act as a ‘data processor’ under the instruction of the CCG and will not process personal data in any manner or for any purpose that is not agreed with the CCG.

The SLA/information sharing agreement will include the core purposes for processing data, as well as key principles and methods compliant with Caldicott principles to only use personal data when necessary and to use the minimum amount of personal data.

# 8 Monitoring providers

As a commissioner of services, the CCG will establish a monitoring process to identify compliance levels within their commissioned providers. This will be via the IG toolkit and where required further discussion and investigation of provider compliance. This will also include ensuring providers are investigating, managing, reporting and publishing details on incidents appropriately.

Any monitoring activity will link to and utilise the NICE Quality Standard 15 (Patient experience statements in adult NHS services) in particular statement 12 related to information exchange.

# 9 Risk, Incident and Query Management

## 9.1 Risk Management methodology:

It is important to define the difference between a risk and an incident. In terms of this methodology, a risk is where a problem has been identified that could lead to an incident. Defining a problem as a ‘risk’ allows for either corrective action, or documented acceptance of that risk to be in place prior to any potential incident and where possible the probability of or impact from an incident to be reduced. The methodology applied is consistent with the general approach to risk management within the organisation.

**Identification of risks:** There are several ways in which a risk will be identified:

- Query raised by staff member
- Assessment of new service or system by information governance team
- Compliance audit by information governance team
- Investigation of an incident/near miss that identifies where risk remains

**Assessment of risks:** Where a risk has been identified in any of the above situations, assessment of the risk will be undertaken by information governance support. The level of documentation on these assessments will vary depending on the situation where the 'risk' has been identified. Risks will be assessed on the '5 x 5' matrix of probability and impact, defined in the organisation risk management policy and utilising the following guidance on potential impacts:

| Level 1 | Level 2 | Level 3 | Level 4 | Level 5 |
|---|---|---|---|---|
| Minor non compliance with standards | Non compliance with standards | Non compliance with core standards | Enforcement action or fine. Major or repeated non compliance with core standards | Prosecution/severe fine. Severely critical report |

- Query – in many cases the advice provided in response to a query will mitigate the risk either entirely or to a reasonable degree. Responses to queries other than those that can be easily answered will be logged by the IG team. Should any real risk remain following the response, this will be included in the log and a risk assessment entered as a 'compliance' risk on the risk register.

- Assessment of new service or system – as with queries, advice provided should mitigate risk entirely or as far as reasonably possible. Should risk remain it will be assessed and where necessary highlighted in either the project risk log or the overall risk register.

- Compliance audit – any audit activity will produce a report that will highlight risks if necessary and potential action to reduce risk. Where the audit activity is part of formal internal or external audit, the formal audit processes will monitor activity to reduce risk and will liaise about appropriate entry in risk registers. Where audit has been undertaken by the information governance team, a report will be produced and any risks included on the risk register until they have been reduced.

- Investigation of an incident or near miss – as with the process to manage incidents the risk will be assessed and reduction actions planned. The process will see the risk reported to the Risk Manager for inclusion in the risk register.

**Reporting of risks:** The majority of risks raised to the information governance team to assess will come from the department that will 'own' the risk and will be seeking 'expert' assessment. Therefore inclusion in the relevant risk register is the responsibility of the staff member reporting the risk. This will be re-iterated by the information governance team when assessing the risk.

Where the information governance team identify, potentially through pro-active audit activity, risks that otherwise might not be identified, they will ensure that the relevant manager in the department is made aware of the risk, in order that it can be included in departmental or corporate risk registers where appropriate.

**Reporting to the SIRO:** Any risk scoring over 8, will be reported to the Senior Information Risk Owner. Risks scoring over 15 should be reported immediately to the SIRO, the Head of Business Intelligence & Informatics and the organisation Risk Manager. Any risk scoring 25 will be reported immediately, via the SIRO to the Chief Executive, or direct in the absence of the SIRO. Risks scoring less than 8 will not be routinely reported.

## 9.2 Incident reporting, management & investigation

**Incident reporting:** The reporting of incidents relating to issues about information is part of the organisation's general 'incident reporting' procedure. Regular information governance education informs all staff to report issues relating to information via the organisation incident reporting process.

**Incident management:** Management of any incident will require collaboration between the risk manager and information governance team. Each incident is specific and will require its own management plan, however there are some forms of incident where swift action is necessary and the information governance team may assume a lead role in management.

- **Allegation or suspected misuse of systems:** It can be vital that potential evidence is preserved. If a case of potential misuse is brought to the attention of the information governance team, they will assess and determine if action is necessary to prevent further user access to system(s) and for IT equipment to be removed from further use for potential forensic examination. As expertise to undertake a forensic examination is limited, the engagement of professional services (NHS Forensic Computing Unit) will be considered. Decision will be taken by the Head of Information Governance and or Senior Information Governance Manager, or in absence by either the Head of IT Services, Head of Consortium or a Chief Officer of the CCG. This is most likely in cases of email, internet or office systems misuse. If a member of staff may be potentially suspended from duty, discussion will take place with HR to determine if access should be temporarily halted, prior to discussion about suspension. Once suspension is confirmed access must be halted to all systems immediately.

- **Data loss/inappropriate disclosure/data inaccuracy:** Where an issue relating to data is reported the Information Governance team will undertake an immediate assessment and determine any potential containment actions. Following all efforts to contain an incident, an initial classification in relation to the published 'Serious Incident Requiring Investigation' scale will be established. Any incidents with an initial classification of 1 or more will be notified to the Senior Information Risk Owner immediately.

  Where classification is difficult due to a lack of facts about a case, a 'worst case scenario' will be established and scored and if appropriate (i.e. level 1 or greater) the SIRO will be informed. The SIRO will determine if the incident should be reported or whether further time will be allowed to establish facts. Reporting will be done by the IG Incident reporting tool in the IG toolkit.

  The Information Governance team will endeavour to establish a realistic score within one working day, depending on the availability of staff involved to answer questions relating to the loss.

  **Informing individuals affected:** Where an incident has either, a potential or direct impact on individuals, then the individuals will be informed. An explanation and apology will be provided. Where possible each person will be contacted individually, unless this will put a significant undue burden on resources and where other methods (i.e. via press release/local media) can be used. Individuals will be contacted by default unless there is a robust reason where informing will cause more harm and distress.

**Incident investigation:** The Information Governance team will utilise the 'Information Security incident' investigation procedure. In addition to scoring on a level as per the risk assessment, the investigation procedure will categorise the impact in relation to the category set in the CRAMM (Computerised Risk Assessment and Management Methodology) tool.

**Incident publication:** Any incident classed as level 2 will be logged on the IG toolkit incident reporting tool. When concluded these will be closed and therefore open to publication by HSCIC. In addition a statement on incidents will be included in the annual CCG statement of control.

## 10 Access control & data transfer principles

The fundamental risks to data are the risks of inappropriate disclosure or unavailability (temporary or permanent). If either of these risks are manifest to a significant degree, public confidence in organisations can be severely damaged, as witnessed since significant 'losses' of data became front page headlines from November 2007. The following strategic approaches to accessing and transferring data are promoted:

- Access on a 'need to know' basis determined where possible by job role, location, organisational structure and where appropriate a care relationship with the patient. These to be determined by the Information Asset Owner.
- Access control systems to support audit of accesses made.
- Storage of data to be on central servers accessed by a network of connected devices, to reduce the need to copy data 'off network'.
- Data taken 'off network' to be encrypted if it contains personal identifiable data or is classed as organisationally sensitive.
- Technical controls over removal of data from network including restriction to organisation owned devices, and authorisation of copying to CD/DVD.
- Secure methods of transfer including NHSMail, encryption and secure file transfer tools to be used. Assessment of paper based transfers such as fax and post via information flow mapping reviews.

## 11 New developments – ensuring compliance

The organisation will ensure that all service development plans (including service re-design), system development plans and other activities that may use personal data will be reviewed to ensure compliance with relevant legislation. This will include both new activities and new ways of working. The organisation will operate a process, in line with the 'Privacy Impact Assessment' from the Information Commissioner's Office to assess and advise on how information should be obtained, stored, used, retained and disposed of in the lifecycle of any activity. It will be a formal requirement of any project to ensure consultation has taken place with Information Governance staff.

## 12 Education Strategy

### Background and Current Position

The headline data losses that started in 2007/08 resulted in a number of central government and ombudsman reports requiring organisations:

*'review and enhance the training that they give to their staff' (ICO report July 08)*

*'to roll out a basic level of mandatory training to all users of personal data, to be completed on appointment and annually' (O'Donnell report June 08)*

### Responsibility for education programme

The Information Governance Team are responsible for the design, implementation and integration of the education items described in this strategy. This is linked to the workforce development leads within the organisation. The IG toolkit assessment requirements will be used to monitor the implementation of education activities.

### Induction

Upon employment all staff will receive an 'acceptable use' email and will undertake the 'online assessment' on core information governance responsibilities. This will be used to raise awareness and measure their current level of knowledge.

It is organisational choice whether their staff will receive an inductions session as soon as possible after starting employment. This will run for 15 minutes in length. The intended outcomes are to:

Ensure staff are aware of the importance of handling information appropriately

Are aware how support and guidance can be accessed

Are aware of the key policy statements they must comply with

This will be by a facilitated presentation, supported by effective handout materials.

### Annual requirement

All directives, whether they come from government investigatory reports, or the IG toolkit make a strong case to provided IG education on an annual basis. Furthermore, there are growing requirements to evidence that the education is inclusive, effective, tailored and regularly reviewed. Below is the revised programme to be provided.

**Assessment and self-directed improvement:**

The minimum requirement for each member of staff is to undertake an annual assessment to prove they have a minimum level of knowledge. This is via the 'Online assessment' set up on the Managed Learning Environment. This links to the online 'code of conduct'. Staff are expected to achieve a minimum of 70% score to pass the module. Re-takes are allowed and staff advised to use online materials to self-direct their learning if they are struggling.

**Further educational support:**

Other items, including those below, will be available on request:

Face to face 'Core information Governance' – as required for those unable to take online training

Patient access requests & information rights – if applicable to those CCG staff members who handle personal confidential data.

Information Assets, data flows & risk assessment (can be delivered as group or by 1-1 facilitated work with information asset owner

Specific team briefs – this will cover topics such as new processing and uses of data, records management and Freedom of Information

**Face to face Core Information Governance**

These sessions will run for approximately 2 hours and will be provided when there is identified demand. Attendance will be for 20 staff (overbooked to 25 in case of drop off). Below is a list of topics, these can be tweaked if a session is being specifically delivered for patient facing or non patient facing roles. All sessions will be interactive and guided by the requirements of the attendees, therefore tailored to their requirements 'on the go'.

Topics covered include:

- Definitions – confidentiality, personal, sensitive
- Legal fundamentals – data protection, freedom of information & other legislation
- Key principles – informing, protecting, sharing, necessity, proportionality
- Consent, public interest, legal duties – in relation to sharing information
- Individual rights
- The fundamentals and benefits/impacts of quality and accuracy
- Key checks on accuracy, managing errors
- The spectrum of uses of data in the service
- Why information needs to be secured, the perils of information loss/unavailability
- The balancing act when protecting information,
- Key security requirements – re mobile working, media, storage, acceptable use, phones, faxes, emails, physical security
- Monitoring, personal use
- Passwords and PINs
- What is a record? Record legislation including Freedom of Information
- Access to records – personal and organisational (inc Subject Access & Freedom Of Information)
- Filing and maintaining effective records
- Retention and destruction

There is a requirement in the IG toolkit to provide education tailored to staff groups. This will be met as it is already by ensuring all sessions are facilitated education sessions, rather than formal training sessions with rigid content. The facilitators will ensure that the discussion and group work is angled to the roles of the staff present as much as possible and invite specific participation.

## Other educational activities

As well as the above facilitated sessions the following activities will support staff education:

All user emails on specific topics, authored by key Directors/Managers

Publicity materials for items such as memory sticks, printing, faxes etc

Screensavers

Sessions at team/department meetings on request (or as result of incident resolution)

Use of products such as the National (CfH) IG training tool, that provide on line learning opportunities. It is noted that the current modules may well be suitable for staff who have specific additional responsibilities, such as the Senior Information Risk Owner and the Information Asset Owners.

## 13 South Central & West Commissioning Support Unit

Information Management and Technology services to the organisation are provided by the South Central & West Commissioning Support (SWCSU), which includes a team focussed on Information Governance. Resources within this team are determined by the Service Level Agreement with SCWCSU and workplan agreed with the Chief Financial Officer and Caldicott Guardian

A lead individual in the Information Governance team will be identified to fulfil the role of ‘Information Governance Manager’ for the organisation.

In order to maintain a quality service of ‘accessible expertise’, all staff within the IG team who fulfil the role of ‘Information Governance Manager’ will be ISEB qualified data protection practitioners (or equivalent) and the team will hold information security related qualifications/training (ISO27000 series)

The IG team will provide support in both pro-active and reactive ways:

- Education – pro-actively through an ongoing programme of mandatory sessions and re-actively to incident reports and queries
- Audit – to meet requirements placed on the organisation by the Department of Health and any local audit procedure and to continually develop and maintain a programme of pro-active compliance audit with policy and procedure within the information risk management programme.
- Expert support – to service and system development programmes

## 14 Development, approval and implementation of guidance

In order to support education programmes and staff queries, the IG team produce a number of guidance documents related to handling information. The following is the core process for development, approval and implementation:

- Guidance will be developed by the team following identification of a significant need. It will draw from sources available at the time including areas such as the Office of the Information Commissioner, the Ministry of Justice and British Standards Institute.
- Following initial draft, key stakeholders across the organisation will be invited to comment
- Final drafts will be put to the CFO and Caldicott Guardian to determine if they need formal approval by the Quality & Governance Committee.
- Finalised guidance will be distributed to each base and General Practice (if appropriate) and included in the Information Governance Reference Pack.
- Awareness will be raised via management channels, as appropriate to the subject and any degree of urgency. Methods will include induction and mandatory education sessions and ‘all staff’ communications.
- If required a specific awareness/implementation programme will be established, the need will be determined by the Information Governance Steering Group.