UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST
BOARD OF DIRECTORS
THURSDAY 30TH MARCH 2017

Title:	**INFORMATION GOVERNANCE TOOLKIT ASSESSMENT**
Responsible Director:	David Burbridge, Director of Corporate Affairs
Contact:	Jodie Haddon-Garrick, Senior Manager Information Governance, Ext 13671

Purpose:	To inform the Board of Directors of the changes to the Information Governance Management Framework (IGMF) and the Trust's self-assessed score for the Information Governance Toolkit Assessment for 2016-2017.	
Confidentiality Level & Reason:	None	
Annual Plan Ref:	Deliver an effective governance and assurance system for regulatory requirements.2.4	
Key Issues Summary:	The Trust has carried out its annual self-assessment against the Information Governance Toolkit. The overall result for 2016 - 2017 is 70% with a mark of satisfactory. The Trust answered all 45 requirements and achieved level 2 or above for all requirements.	
Recommendations:	The Board of Directors is asked to: 1 approve the Information Governance Management Framework; and 2 agree that the Trust submits a score of 70% for the 2016 -17 Information Governance Toolkit assessment.	
Approved by:	David Burbridge	March 2017

UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST

BOARD OF DIRECTORS
THURDSAY 30TH MARCH 2017

INFORMATION GOVERNANCE TOOLKIT ASSESSMENT

PRESENTED BY THE DIRECTOR OF CORPORATE AFFAIRS

1. Introduction

The purpose of this paper is to:

1.1. inform the Board of Directors of the Trust's score for the Information Governance Toolkit Assessment for 2016-2017 (Version 14) and all changes to the Information Governance Management Framework (IGMF); and

1.2. ask the Board to approve the:

1.2.1. Assessment prior to its final submission to HSCIC and

1.2.2. revised Information Governance Management Framework (IGMF).

2. Background to the Information Governance Toolkit

2.1. Since 16 September 2009 it is a requirement for all NHS Trusts to complete an Information Governance Toolkit (IGT) self-assessment annually and to submit the same to HSCIC at the end of each financial year.

2.2. The Audit Committee receives an annual report on the overall process. Since 2015/16 there is a new mandatory requirement to have the IG Toolkit assessment audited by the Trust's Internal Auditors. Both, the annual IGT process report and the draft Internal Audit Report were presented to the Audit Committee at the March meeting. The final Internal Audit Report will be presented to the May meeting. The IGT process has been given 'significant assurance with minor improvement opportunities'.

2.3. Version 14 of the IGT consists of 45 requirements. For each requirement the Trust must self-assess and provide a score. Scoring is on a basis of level 0 up to Level 3, with 3 being the highest.

2.4. The overall score is displayed as a percentage and also marked as satisfactory or unsatisfactory. To achieve an overall satisfactory mark the Trust is required to achieve level 2 for all 45 requirements.

3. **Result for the Information Governance Toolkit Assessment for 2016/2017 (Version 14)**

3.1. The overall result for 2016 - 2017 (Version 14 Assessment) is 70% with a mark of 'satisfactory' compared to 72% for 2015 – 2016 (see also table 1 and 2 below). The Trust answered all 45 requirements. The Trust achieved level 2 or above for all requirements. For a full breakdown please refer to Appendix 1.

3.2. There has been a slight decrease in the overall score by 2% points. An updated version of the Toolkit is produced each year which renders it difficult to make a reliable comparison with scores from previous assessments. In addition, the evidence required to achieve the attainment levels varies year on year, where level 3 has been achieved previously additional evidence is required to maintain that level, which the Trust may not have. For 2016 - 2017 it was necessary to reduce some requirements relating to health records, information security and training from a level 3 to a level 2. The withdrawal of the IG Training Tool website from November onwards has had an impact on scoring as courses such as the SIRO and IAO training were no longer available. On the other hand, the requirement in relation to the Freedom of Information Act has been upgraded from a level 2 to a level 3.

Table 1: Comparison of number of requirements at each level

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Total Requirements	Overall Score	Current Grade
Version 11 (2013 – 14)	Published	0	0	26	19	45	80%	Satisfactory
Version 12 (2014 – 15)	Published	0	0	32	13	45	76%	Satisfactory
Version 13 (2015 – 16)	Published	0	0	37	8	45	72%	Satisfactory
Version 14 2016-2917	Current	0	0	40	5	45	70%	Satisfactory

Table 2: Comparison of previous IGT scores

Year of IG assessment	Score
Version 14 2016-17	70%
Version 13 2015-16	72%
Version 12 2014-15	76%
Version 11 2013-14	80%
Version 10 2012-13	80%
Version 9 2011-12	77%
Version 8 2010-11	77%
Version 7 2009-10	80%
Version 6 2008-09	79%
Version 5 2007-08	81%
Version 4 2006-07	89%
Version 3 2005-06	92%

Version 2 2004-05	90%
Version 1 2003-04	76%

6. Review of the Information Governance Framework (IGMF)

6.1 The Trust is required to undertake an annual review of the Information Governance Management Framework (IGMF). To achieve level 3 for requirement 101 IGT this document must be reviewed by the Board.

6.2 The Framework has been reviewed and approved at the Information Governance Group. The Framework is attached at Appendix 2 with the most significant changes marked in red. Changes include a new monitoring matrix (similar to that used for policies), a new strategy implementation section and a revised policy/procedure table.

7. Information Governance Assurance Statement

7.1 All organisations submitting an IG Toolkit assessment are required to accept the Information Governance Assurance Statement. Acceptance automatically occurs at the point of submission.

7.2 The full statement can be viewed at Appendix 3.

8. Recommendations

The Board of Directors is asked to:

8.1 approve the Information Governance Framework; and

8.2 agree that the Trust submits a score of 70% for the 2016 -17 Information Governance Toolkit assessment (Version 14).

David Burbridge
Director of Corporate Affairs **March 2017**

Appendix 1

IG Toolkit Completed Assessment

Version 14 (2016 -2017) Assessment Requirements List

14-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	Level 3
14-201	The organisation ensures that arrangements are in place to support and promote information sharing for coordinated and integrated care, and staff are provided with clear guidance on sharing information for care in an effective, secure and safe manner	Level 2
14-202	Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected	Level 2
14-203	Patients, service users and the public understand how personal information is used and shared for both direct and non-direct care, and are fully informed of their rights in relation to such use	Level 2
14-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Level 3
14-206	Staff access to confidential personal information is monitored and audited. Where care records are held electronically, audit trail details about access to a record can be made available to the individual concerned on request	Level 2
14-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Level 2
14-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Level 2
14-210	All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements	Level 2
14-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Level 2
14-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Level 2
14-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Level 2

14-303	There are established business processes and procedures that satisfy the organisation’s obligations as a Registration Authority	Level 2
14-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	Level 2
14-305	Operating and application information systems (under the organisation’s control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems	Level 2
14-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation’s information risk policy and information risk management strategy	Level 2
14-308	All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers	Level 2
14-309	Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place	Level 2
14-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Level 2
14-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	Level 2
14-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Level 2
14-314	Policy and procedures ensure that mobile computing and teleworking are secure	Level 2
14-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Level 2
14-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Level 2
14-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Level 2
14-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Level 2
14-402	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care	Level 2

14-404	A multi-professional audit of clinical records across all specialties has been undertaken	Level 2
14-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Level 2
14-501	National data definitions, standards, values and data quality checks are incorporated within key systems and local documentation is updated as standards develop	Level 2
14-502	External data quality reports are used for monitoring and improving data quality	Level 2
14-504	Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained	Level 2
14-505	An audit of clinical coding, based on national standards, has been undertaken by a Clinical Classifications Service (CCS) approved clinical coding auditor within the last 12 months	Level 2
14-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Level 2
14-507	The secondary uses data quality assurance checks have been completed	Level 2
14-508	Clinical/care staff are involved in quality checking information derived from the recording of clinical/care activity	Level 2
14-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	Level 2
14-601	Documented and implemented procedures are in place for the effective management of corporate records	Level 2
14-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Level 3
14-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Level 2

Appendix 2

University Hospitals Birmingham NHS
NHS Foundation Trust

Information Governance Management Framework and Strategy

1. Introduction

a. Information is vital for the Trust. It supports the day to day clinical operations, as well as the effective management of services and resources. Information Governance therefore has to strike the appropriate balance between openness and confidentiality in order to deliver high quality health care.

b. Furthermore, Information Governance has to ensure that information is treated within the legal framework of the Data Protection Act 1998, Freedom of Information Act 2000, Computer Misuse Act 1990, Prevention of Terrorism Act 2005, Caldicott principles, common law duty of confidentiality and numerous other acts, regulations and guidance documents (see Annex I). These dictate that information has to be obtained fairly and efficiently, held securely and confidentially, recorded accurately and reliably, used effectively and ethically, and shared appropriately and lawfully.

c. Information Governance therefore requires a framework of clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources which are further described in this document.

2. Objectives

a. The Information Governance Framework supports the following objectives:

i. Openness
ii. Legal compliance
iii. Information security
iv. Information quality assurance
v. Proactive use of information

b. <u>Openness</u>

i. The Trust holds a variety of information. Some of the information is personal to the Trust’s service users, their families and its staff. This information is confidential and requires adequate protection from illegal/inappropriate access. Other information might be commercially sensitive which also requires appropriate protection. A third category of information refers to information which is neither personal nor otherwise confidential. This includes but is not limited to information about the

Trust's services and treatment options. This information must be available to the public through a variety of media, in line with the current legal framework.

ii. The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000 and Environmental Information Regulations.

iii. The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness.

iv. The Trust will ensure that patients have ready access to information relating to their own health care, their options for treatment and their rights as patients.

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

vi. The Trust will have clear procedures and arrangements for subject access requests from patients and the public.

c. The Trust will include details of any serious untoward incidents associated with information governance within its public Annual Report.

d. The Trust will provide assurances as to the processes for managing Information Governance in a sound and robust way within its Annual Governance Statement.

e. Legal Compliance

i. The Trust regards all identifiable personal information relating to patients as confidential.

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

iii. The Trust will establish and maintain policies to ensure compliance with the Data Protection Act 2000, Human Rights Act 1998, the Common Law Duty of Confidentiality, the Caldicott Principles and any other relevant law.

iv. 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, Crime and Disorder Act, Protection of Children Act).

f. Information Security

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

ii. The Trust will undertake or commission assessments and audits of its information and IT security arrangements.

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

iv. The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security in line with the Data Protection Incident Management Standard Operating Procedure. All staff will be informed of the reporting process during Information Governance mandatory training.

v. The Trust will integrate the requirement for information security management system policies into its procurement processes as appropriate.

g. Information Quality Assurance

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

ii. The Trust will undertake or commission assessments and audits of its information quality and records management arrangements.

iii. Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

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

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

vi. The Trust will promote information quality and effective records management through policies, procedures/user manuals and training.

3. Trust Values

a. The Information Governance Framework supports the following Trust values:

- Respect
- Responsibility
- Honesty
- Innovation

b. Respect

The Trust will respect the wishes of patients, colleagues, visitors and carers by ensuring confidential information is handled in accordance with relevant law, policies and procedures.

c. Responsibility

By effectively planning and managing Information Governance, the Trust aims to ensure that individual staff take responsibility to protect confidential information. Furthermore, the accountability structure for Information Governance ensures that the Trust also takes collective responsibility for the overall strategy and monitoring of protecting information.

d. Honesty

The Trust ensures openness and honesty with our engagement and decision-making processes and ensures that the policies and practice reflect this.

e. Innovation

In order to look for more efficient and effective ways to deliver services and improve patient outcomes, the Trust strives to be innovative. The Trust therefore has robust processes in place to monitor the effect any changes may have on the way in which confidential information is handled.

4. Controls

a. The Trust's Information Governance objectives are inherently linked to the key risks recorded on the Information Governance risk register. The Trust relies on a variety of controls to mitigate these risks which are at the same time the deliverables which support the achievement of the aforementioned key objectives. In the following the document simply refers to controls. These controls encompass the following:

i. Policies and procedures
ii. IG Toolkit controls (including assessment)
iii. Training and awareness
iv. IG related contractual clauses

b. Policies and procedures

Policy / Procedure	Date of Approval	Approving Body	Review date
Information Governance Policy	01/01/15	BoD	01/01/2018
Data Protection & Confidentiality Policy	01/01/15	CEAG	01/01/2018
Information Security Policy	16/09/14	CEAG	16/09/2017
Records Management & Information Lifecycle Policy	28/01/15	CEAG	01/01/2018
Freedom of Information Act and Environmental Information Regulations Policy	01/04/16	CEAG	01/03/2019
Corporate Governance Policy	28/03/13	BoD	28/02/2016
Policy for the Reporting and Management of Incidents including Serious Incidents Requiring Investigation	01/03/17	CEO	01/03/2020
Procedure for the Reporting and Management of Incidents Including Serious Incidents Requiring Investigation	24/11/2014	DCA	01/06/2016
IG Incident Management SOP	04/03/2016	IGG	03/03/2019
IT Acceptable Use Policy (new)	27/10/2016	BOD	26/10/2019
Subject Access Request Procedure	Awaiting approval	DCA	
Information Asset Register Procedure	09/12/2016	DCA	08/12/2018
Information Privacy Impact Assessment Procedure	09/12/2016	DCA	08/12/2017
ISMS Risk assessment	17/06/15	IT	16/06/2018

c. IG Toolkit controls (including assessment)

i. The IG Toolkit mandates a great number of controls which further mitigate the key information governance risks. This includes but is not limited to the data mapping tool, information risk assessments, information asset register and a robust privacy impact assessment process.

ii. The annual Information Governance Toolkit assessment is completed by the Information Governance team working with relevant departments throughout the Trust. The Trust aims for information governance to be embedded throughout the organisation and therefore works with other departments to develop, implement and monitor policies and procedures. The following Trust services are therefore stakeholders in the submission of the IGT assessment:

- Information Governance
- IT Services and IT Security
- Informatics
- Medical Records
- Corporate Affairs

iii. The stakeholders work together to comply with the following HSCIC timeline for IGT submission:

- Baseline – 31st July
- Performance Submission – 31st October
- Final Submission – 31st March

d. Information Governance Training/Awareness

i. In order to ensure awareness and understanding of Trust Information Governance policies and procedures, all staff are required to attend corporate induction and thereafter annual information governance training. Training is accessible in a number of ways and the Information Governance Training Needs Analysis (Annex II) provides assurance that the right type of information governance training is delivered to the right groups of staff.

ii. In addition to face-to-face or video teaching in classrooms and lecture theatres, the Trust asks staff to utilise the on-line HSCIC information governance training tool.

e. IG related contractual clauses

i. Confidentiality clauses are included in staff contracts of employment.

ii. Non-disclosure agreements are used where commercially sensitive information is shared with third parties.

iii. Appropriate data sharing/processing agreements are used with third-parties.

5. Monitoring and Assurance

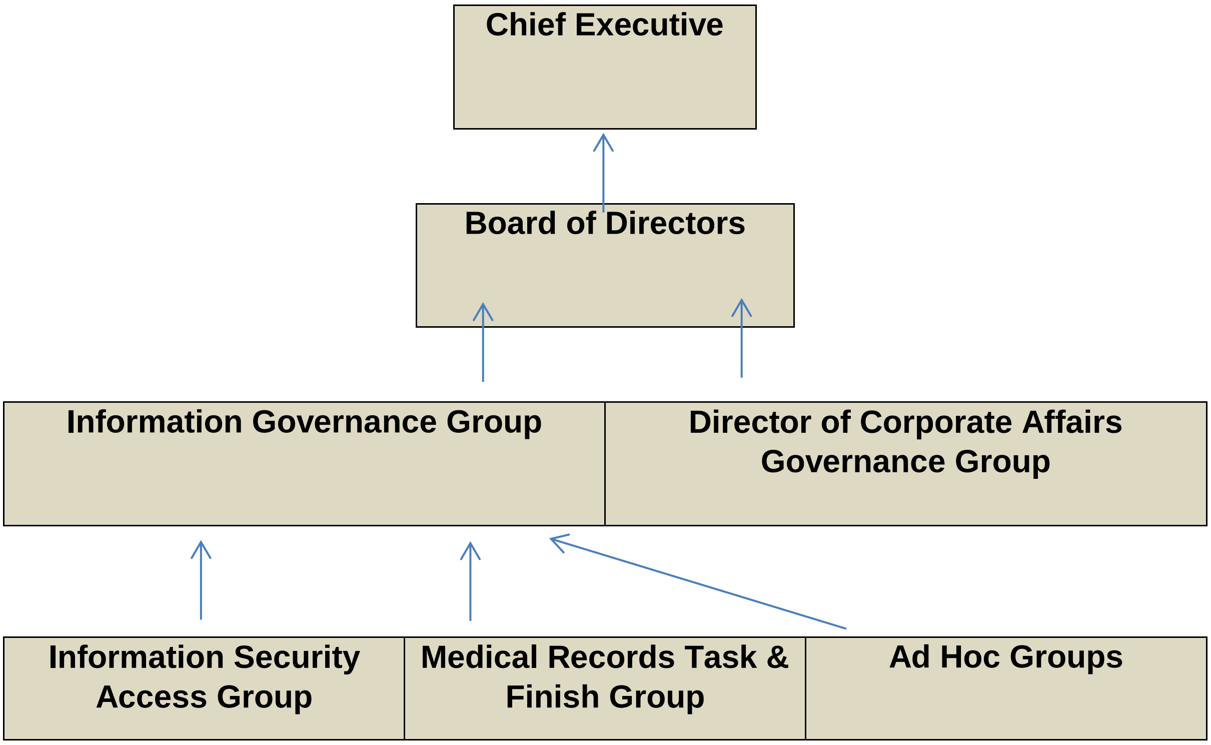
Control	Assurance	Assurance Source	Responsible	Action
Policies/procedures (in general)	Policies and procedures are fit for purpose, have been appropriately reviewed with stakeholders and approved in line with the Controlled Document Policy and Procedure	IGG/ISAG minutes PRG minutes BOD/CEAG minutes	Senior Manager Information Governance	Continue to review and update IG related policies and procedures
Policy audits	Compliance with IG related policies (e.g. IG; IT Acceptable Use; FOI)	DCA Governance Group report and minutes	Corporate Affairs Officer	Carry out audits in accordance with overall policy audit programme
Training and awareness	Compliance with staff training in line with IG Toolkit requirements and Trust training policies	DCQG report and minutes IGG report and minutes	Senior Manager Information Governance	Produce quarterly reports
IG related contract clauses with third parties	SOP with procurement (to be developed); audit programme (to be established)	Report to DCA Governance Group (to be developed)	Senior Manager Information Governance	Develop SOP and audit programme
Consent audits	Ensure consent to treatment/access to information has been given in accordance with the law	IGG report (to be developed)	IG Officer	Review the consent process given the changes under the GDPR; develop audit programme

Data mapping tool	Ensure data is shared in accordance with IG law and related Trust policies	IG Toolkit assessment Annual reports to SIRO	IG Officer	Complete annual report to SIRO
Information risk assessments	Ensure that information is handled in accordance with IG law and related Trust policies	Report to SIRO	IG Officer	Complete annual report to SIRO
Information Asset Register	Ensure that responsibility for the physical and technical security of information is owned and risk managed by named senior employees	Report to SIRO	IG Officer	Complete annual report to SIRO
Privacy Impact Assessments	Ensure that privacy is embedded in Trust processes and projects	Minutes of EPR/IGG	IG Officer	Promote use of PIAs
Incident management	Ensures consequences are handled, investigated and prevented appropriately in accordance with ICO requirements	DCQG report and minutes IGG report and minutes	IG Officer	Continue to raise incident reporting awareness
User Access Control	Ensures that only correct people have access to information in accordance with relevant legislation and Trust policies	Report to/minutes of ISAG	Senior Manager Information Governance	Review and update 'User Access Control Policy'

Further details of the Information Governance Framework are included in the Information Governance Policy.

6. Accountability and responsibility

a. The Chief Executive Officer takes ultimate responsibility for information governance throughout the Trust and receives assurance regarding information governance compliance from the Board. The Information Governance Group and Director of Corporate Affairs Governance Group both report to the Board. The structure is outlined in below:


Chief Executive
Board of Directors
Information Governance Group
Director of Corporate Affairs Governance Group
Information Security Access Group
Medical Records Task & Finish Group
Ad Hoc Groups

b. The Caldicott Function

i. The Caldicott Guardian in the Trust provides an advisory role to the organisation to ensure the Trust safeguards patients' best interests by both the protecting their confidentiality and disclosing their information when appropriate. This role is filled by the Trust Medical Director.

ii. The Medical Director is supported and resourced by other members of staff who assist in the performance of the Caldicott Function:

- Deputy Director of Corporate Affairs, Legal & Risk
- Associate Foundation Secretary

- Senior Information Governance Manager
- Information Governance Officer
- Information Governance Assistant
- IT Security Manager
- Health Records Services Manager

c. The SIRO

i. The Senior Information Risk Owner (SIRO) in the Trust is responsible for ensuring organisational information risk is properly identified and managed and that appropriate assurance mechanisms exist. To enable this to happen, the SIRO has the following responsibilities:

- Fosters a corporate culture that values, protects and uses information for the success of the organisation and benefit of its patients;
- Owns the organisation's overall information risk policy and risk assessment processes and ensures they are implemented consistently by IAOs;
- Advisers the CEO on the information risk aspects of their statement on internal controls; and
- Owns the Trust data protection incident management process.

ii. The Trust SIRO is the Director of Corporate Affairs and in their role as a Board member, this ensures that information governance remains at a suitably high level in the Trust.

iii. The SIRO is supported by Information Asset Owners who are directly accountable to the SIRO for providing assurance that information risk is managed effectively for the information assets that they have responsibility for. Information Asset Administrators manage the day-to-day running of the information assets and are accountable to the Asset Owners.

iv. Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the Trust.

d. Governance Bodies

In addition to individual roles which support the information governance agenda, the Trust has a number of groups which take responsibility for information governance:

- Policy Review Group (PRG)
- Board of Directors (BoD)
- Chief Executive Advisory Group (CEAG)

- Information Governance Group (IGG)
- Director of Corporate Affairs Governance Group (DCA GG)
- Information Security Advisory Group (ISAG)
- Medical Records Task & Finish Group
- Data Quality Group (DQG)

e. All staff

All staff (whether permanent, temporary, contractors or volunteers) are responsible for ensuring compliance with Trust Information Governance Policies and Procedures.

7. Strategy implementation

a. The Information Governance Group (IGG) will monitor overall implementation of this strategy and its associated work streams through quarterly meetings and through its IG sub-groups (ISAG; Access Group).

b. Each group shall have its own minutes and/or action matrices where progress shall be tracked.

c. ISAG will review the risk assessments and information asset register before they are submitted for their annual review by the SIRO. ISAG will further review any audits carried out in support of the IG objectives.

d. IGG will complete its self-assessment as outlined above and provide an overview of progress being made to the Audit Committee and/or Board as agreed in their annual cycles.

e. IGG will review this strategy annually or in response to any significant changes in legislation or regulation, national guidance or significant information governance breaches.

Reviewed	14th March 2017
Approved	14th March 2017 – Information Governance Group
Review Date	March 2018

Annex I – Relevant Law

DATA PROTECTION ACT 1998

Processing of Personal Data must comply with the eight data protection principles of the Data Protection Act 1998. This includes all processing of Personal Data which falls within the scope of this Agreement.

The parties to this Agreement must have a data protection notification which includes the purposes documented in Section 2 and sources/disclosures to the parties listed in Section 1.

HUMAN RIGHTS ACT 1998

Article 8.1 of the European Convention on Human Rights enshrined in Schedule 1 of the Human Rights Act 1998, provides that "*everyone has the right to respect for his private and family life, his home and his correspondence.*" This is however, qualified by reasons where it may be legitimate to infringe this right. As stated in Article 8.2, these are "*in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The right to privacy will be respected by parties to this Agreement unless it can be shown that there is a legitimate reason to infringe those rights.

COMMON LAW DUTY OF CONFIDENTIALITY

The duty of confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence, it must only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm).

Parties to this Agreement will restrict disclosure of confidential information to those purposes that an individual has been informed of and consented to, unless there is a statutory requirement to use that information or a robust public interest justification for it use.

FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act 2000 is intended to promote a culture of openness and accountability amongst public authorities by providing people with rights of access to the information held by public authorities.

From 1 January 2005 each public authority must comply with requests for the information that it holds unless an exemption from disclosure applies.

Where an applicant requests their own personal information, mistakenly citing the Freedom of Information Act, the request must be treated as a request under the Data Protection Act.

Where an applicant requests third party information, the request can be refused in certain circumstances. S.7(4) of the Data Protection Act will be the starting point for any consideration of whether the data should, or should not, be disclosed.

The fairness of the disclosure must be assessed against any unnecessary or unjustified damage or distress to that individual, the expectations of an individual that their information would not be disclosed and any refusal of consent to disclose.

THE COMPUTER MISUSE ACT, 1990.

The Computer Misuse Act, 1990 was passed to deal with the problem of hacking of computer systems. In the early days of hacking, the problem wasn't taken very seriously – it was seen as mischievous behaviour, rather than as something which could cause serious loss or problems to companies, organisations and individuals. Before 1990, it was difficult to prosecute people for hacking – existing laws were not written with that in mind. However, it became increasingly clear that hacking should be against the law, and that the laws should be effective and enforceable. As a result, the Computer Misuse Act was passed in 1990.

The Act created three new offences:

- Unauthorised access to computer material

- Unauthorised access with intent to commit or facilitate commission of further offences

- Unauthorised modification of computer material.

THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA)

The Regulation of Investigatory Powers Act 2000 (RIPA) provides for, and regulates the use of, a range of investigative powers, by a variety of public authorities. It updates the law on the interception of communications to take account of technological change such as the growth of the Internet. It also puts other intrusive investigative techniques on a statutory footing for the very first time; provides new powers to help combat the threat posed by rising criminal use of strong encryption; and ensures that there is independent judicial oversight of the powers in the Act.

PREVENTION OF TERRORISM ACT 2005

All citizens, including doctors, must inform police, as soon as possible, of any information that may help to prevent an act of terrorism, or help in apprehending or prosecuting a terrorist.

INFORMATION SECURITY STANDARDS ISO/IEC27001, ISO/IEC17799 AND BS7799

ISO/IEC 27001 2005, ISO/IEC17799:2005 and **BS7799** 2002 are the best practice information security management standards, defining and guiding ISMS developments.

Annex I – Training Needs Analysis

	SIRO	Caldicott Guardian	Senior Manager Information Governance	Assoc. Director for Corporate Affairs, Legal & Risk	Associate Foundation Secretary	Health Records Services Manager	Access to Health Staff	Information Security Manager	EPR Lead	IAOs / IAAs	All Staff
HSCIC Confidentiality & Caldicott Modules											
Patient Confidentiality	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	
The Caldicott Guardian in the NHS and social care		🟦	🟦								
HSCIC Information Governance Management Modules											
Introduction to Information Governance	🟦	🟦	🟦	🟦	🟦			🟦	🟦	🟦	
HSCIC Information Risk Management Modules											
NHS Information Risk Management:	🟦		🟦	🟦	🟦			🟦		🟦	

Introductory	🟦		🟦	🟦	🟦			🟦		🟦	
NHS Information Risk Management: Foundation	🟦		🟦	🟦	🟦			🟦		🟦	
NHS Information Risk Management for SIROs and IAOs	🟦		🟦	🟦	🟦			🟦		🟦	
HSCIC Information Security Modules											
Password Management	🟦	🟦	🟦					🟦	🟦	🟦	
Information Security Guidelines	🟦	🟦	🟦					🟦	🟦	🟦	
Secure Transfers of Personal Data	🟦	🟦	🟦					🟦	🟦	🟦	
Information Security Management	🟦		🟦					🟦		🟦	
Business Continuity Management	🟦		🟦					🟦		🟦	
HSCIC Records Management Modules											

Records Management and the NHS Code of Practice				🟦	🟦	🟦	🟦				
Records Management in the NHS				🟦	🟦	🟦	🟦				
Access to Health Records		🟦	🟦	🟦	🟦	🟦	🟦		🟦		
The Importance of Good Clinical Record Keeping		🟦				🟦	🟦		🟦		
Dilys Jones - The Information Asset Register	🟦		🟦	🟦	🟦			🟦		🟦	
Dilys Jones - Cyber Security	🟦		🟦	🟦	🟦			🟦		🟦	
HSCIC Cyber Security Certificate								🟦			
Subject Access Requests Procedure			🟦	🟦	🟦	🟦	🟦				
Mandatory IG Training	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

Annex II – Relevant Law

DATA PROTECTION ACT 1998

Processing of Personal Data must comply with the eight data protection principles of the Data Protection Act 1998. This includes all processing of Personal Data which falls within the scope of this Agreement.

The parties to this Agreement must have a data protection notification which includes the purposes documented in Section 2 and sources/disclosures to the parties listed in Section 1.

HUMAN RIGHTS ACT 1998

Article 8.1 of the European Convention on Human Rights enshrined in Schedule 1 of the Human Rights Act 1998, provides that "*everyone has the right to respect for his private and family life, his home and his correspondence.*" This is however, qualified by reasons where it may be legitimate to infringe this right. As stated in Article 8.2, these are "*in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*"

The right to privacy will be respected by parties to this Agreement unless it can be shown that there is a legitimate reason to infringe those rights.

COMMON LAW DUTY OF CONFIDENTIALITY

The duty of confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence, it must only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm).

Parties to this Agreement will restrict disclosure of confidential information to those purposes that an individual has been informed of and consented to, unless there is a statutory requirement to use that information or a robust public interest justification for it use.

FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act 2000 is intended to promote a culture of openness and accountability amongst public authorities by providing people with rights of access to the information held by public authorities.

From 1 January 2005 each public authority must comply with requests for the information that it holds unless an exemption from disclosure applies.

Where an applicant requests their own personal information, mistakenly citing the Freedom of Information Act, the request must be treated as a request under the Data Protection Act.

Where an applicant requests third party information, the request can be refused in certain circumstances. S.7(4) of the Data Protection Act will be the starting point for any consideration of whether the data should, or should not, be disclosed.

The fairness of the disclosure must be assessed against any unnecessary or unjustified damage or distress to that individual, the expectations of an individual that their information would not be disclosed and any refusal of consent to disclose.

THE COMPUTER MISUSE ACT 1990.

The Computer Misuse Act, 1990 was passed to deal with the problem of hacking of computer systems. In the early days of hacking, the problem wasn't taken very seriously – it was seen as mischievous behaviour, rather than as something which could cause serious loss or problems to companies, organisations and individuals. Before 1990, it was difficult to prosecute people for hacking – existing laws were not written with that in mind. However, it became increasingly clear that hacking should be against the law, and that the laws should be effective and enforceable. As a result, the Computer Misuse Act was passed in 1990.

The Act created three new offences:

- Unauthorised access to computer material

- Unauthorised access with intent to commit or facilitate commission of further offences

- Unauthorised modification of computer material.

THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA)

The Regulation of Investigatory Powers Act 2000 (RIPA) provides for, and regulates the use of, a range of investigative powers, by a variety of public authorities. It updates the law on the interception of communications to take account of technological change such as the growth of the Internet. It also puts other intrusive investigative techniques on a statutory footing for the very first time; provides new powers to help combat the threat posed by rising criminal use of strong encryption; and ensures that there is independent judicial oversight of the powers in the Act.

PREVENTION OF TERRORISM ACT 2005

All citizens, including doctors, must inform police, as soon as possible, of any information that may help to prevent an act of terrorism, or help in apprehending or prosecuting a terrorist.

INFORMATION SECURITY STANDARDS ISO/IEC27001, ISO/IEC17799 AND BS7799

ISO/IEC 27001 2005, ISO/IEC17799:2005 and **BS7799** 2002 are the best practice information security management standards, defining and guiding ISMS developments.