UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST
BOARD OF DIRECTORS
THURSDAY 24TH MARCH 2016

Title:	**INFORMATION GOVERNANCE TOOLKIT ASSESSMENT**
Responsible Director:	David Burbridge, Director of Corporate Affairs
Contact:	Rachel Seabright, Information Governance Manager, Ext 13707

Purpose:	To inform the Board of Directors of the Trust's self-assessed score for the Information Governance Toolkit Assessment for 2015-2016, to seek approval of the assessment prior to submission and to approve the Information Governance Management Framework.	
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 2015 - 2016 is 72% 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 72% for the 2015 -16 Information Governance Toolkit assessment.	
Approved by:	David Burbridge	March 2016

UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST

BOARD OF DIRECTORS
THURDSAY 24TH MARCH 2016

INFORMATION GOVERNANCE TOOLKIT ASSESSMENT

PRESENTED BY THE DIRECTOR OF CORPORATE AFFAIRS

1. **Introduction**

The purpose of this paper is to inform the Board of Directors of the Trust's score for the Information Governance Toolkit Assessment for 2015-2016 (Version 13) and to ask the Board to approve the assessment prior to final submission of it to HSCIC and to approve the Information Governance Management Framework.

2. **Background to the Information Governance Toolkit**

2.1 The Information Governance Toolkit is a self-assessment completed annually by the Trust and submitted to HSCIC at the end of each financial year.

2.2 Version 13 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.

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

3. **Procedure for scoring of the Information Governance Toolkit**

3.1 The scoring for the requirements is completed by the lead for each area and all evidence is uploaded to Health Assure.

3.2 The Information Governance Manager, Deputy Director for Corporate Affairs, Legal and Risk and the Associate Foundation Secretary have agreed the final scores for the assessment.

3.3 The Board of Directors is asked to agree and sign off the completed assessment.

4. **Result for the Information Governance Toolkit Assessment for 2015/2016 (Version 13)**

4.1 The overall result for 2015 - 2016 (Version 13 Assessment) is 72% with a mark of satisfactory. For a full breakdown please refer to Appendix 1

to this report.

4.2 The Trust answered all 45 requirements.

4.3 The Trust achieved level 2 or above for all requirements.

5 Comparison with previous year's assessment

5.1 The score for the Information Governance Toolkit assessment for 2014 – 2015 was 76% with a mark of satisfactory compared to a score of 72% this year. As an updated version of the Toolkit is produced each year it is 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. Following a complete review of all requirements, it was necessary to reduce some requirements relating to informatics and information/cyber security from a level 3 to a level 2 due to a changing landscape.

5.2 There are other requirements which have been upgraded from a level 2 to a level 3 as a result of the implementation of last year's Information Governance Plan.

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)	Current	0	0	37	8	45	72%	Satisfactory

Comparison of previous scores for Information Governance Toolkit Assessments

Year of IG assessment	Score
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 Information Governance Framework

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

6.2 The Framework has undergone changes this year to satisfy a greater number of requirements of the Toolkit. The Framework is attached at Appendix 2.

7. Information Governance Assurance Statement

7.1 All organisations submitting an IG Toolkit assessment are required to accept the Information Governance Assurance Statement. This happens 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 72% for the 2015 -16 Information Governance Toolkit assessment (Version 13).

David Burbridge
Director of Corporate Affairs **March 2016**

Appendix 1

IG Toolkit Completed Assessment

Version 13 (2015 -2016) Assessment Requirements List

Req No	Description	Score
12-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	**3**
12-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	**3**
12-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	**2**
12-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	**2**
12-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	**3**
12-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	**3**
12-201	Staff are provided with clear guidance on keeping personal information secure, on respecting the confidentiality of service users, and on the duty to share information for care purposes	**2**
12-202	Personal information is shared for care but is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected	**2**
12-203	Individuals are informed about the proposed uses of their personal information	**2**
12-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	**3**
12-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	**2**
12-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	**2**
12-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	**2**
12-210	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	**2**
12-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	**2**
12-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	**2**
12-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	**3**

12-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	**2**
12-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	**2**
12-305	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	**2**
12-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	**3**
12-308	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	**2**
12-309	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	**2**
12-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	**2**
12-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	**2**
12-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	**2**
12-314	Policy and procedures ensure that mobile computing and teleworking are secure	**2**
12-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	**2**
12-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	**2**
12-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	**2**
12-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	**2**
12-402	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care	**2**
12-404	A multi-professional audit of clinical records across all specialties has been undertaken	**2**
12-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	**3**
12-501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	**2**
12-502	External data quality reports are used for monitoring and improving data quality	**2**
12-504	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	**2**

12-505	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	**2**
12-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	**2**
12-507	The Completeness and Validity check for data has been completed and passed	**2**
12-508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	**2**
12-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	**2**
12-601	Documented and implemented procedures are in place for the effective management of corporate records	**2**
12-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	**2**
12-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	**2**

Appendix 2

University Hospitals Birmingham NHS
NHS Foundation Trust

Information Governance Management Framework 2016/17

1. Introduction

The Trust aims to deal with personal and confidential information legally, securely and efficiently to deliver the best possible care to patients and recognises the need for an appropriate balance between openness and confidentiality to ensure the effective management and use of information. Whilst meeting statutory and national obligations to promote openness and public accountability, the Trust seeks to safeguard personal and confidential information. The Trust also recognises the need to share information in a controlled manner with other health and social care providers in the best interests of the patient.

This Management Framework gives assurance that the Trust is meeting these aims within the legal and regulatory framework of information governance. The Trust will establish and maintain policies and procedures to ensure compliance with any relevant law (Appendix II), NHS guidance and requirements contained in the Health and Social Care Information Centres Information Governance Toolkit.

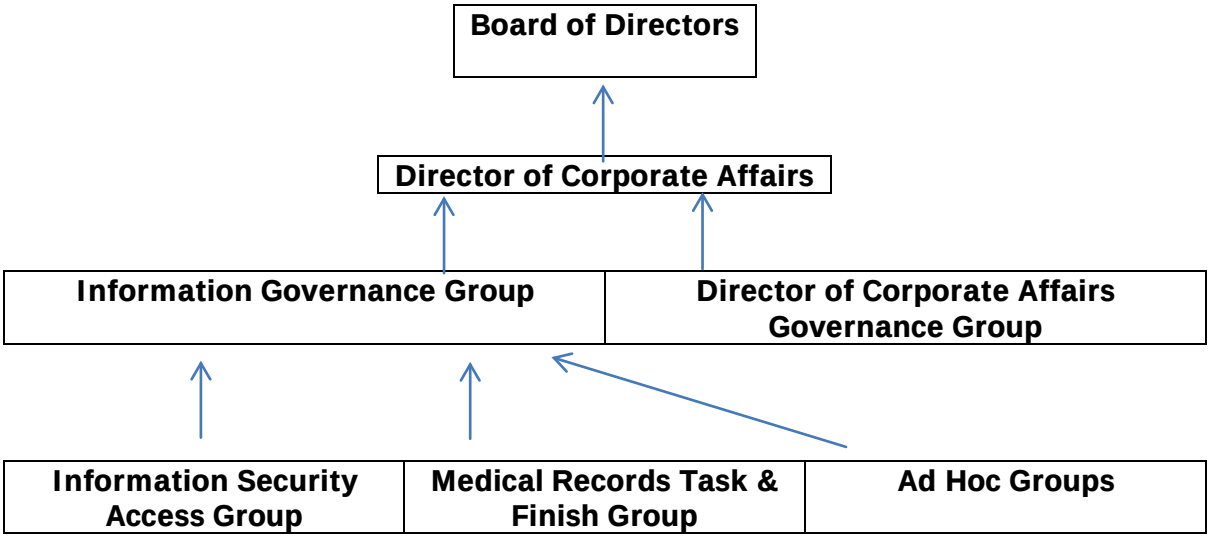
2. Information Governance Objectives

To ensure that the Trust:

- Maintains openness with regards to the information held by the Trust;
- Ensures all information is held safely and securely, and also disclosed, in accordance with the relevant law and national guidance;
- Maintains effective information security of personal and confidential data;
- Maintains information quality assurance across the Trust; and
- Updates annually the Information Governance Toolkit (IGT) in accordance with the Health and Social Care Information Centre timelines.

3. Information Governance Accountability and Framework

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



4. Senior Information Governance Roles

4.1 The Caldicott Function

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

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
- IT Security Manager
- Health Records Services Manager

4.2 The SIRO

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.

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.

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.

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.

4.3. 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)

4.4. All staff

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

5. Information Governance Relevant Policies and Procedures

Policy / Procedure	Date of Approval	Approving Body
Information Governance Policy	01/01/15	BoD
Data Protection & Confidentiality Policy	01/01/15	CEO
Information Security Policy	16/09/14	CEO
Records Management & Information Lifecycle Policy	28/01/15	CEO
Freedom of Information & EIR Policy	19/04/13	CEO
Corporate Governance Policy	01/04/13	BoD
Incident Reporting and Managing Policy	05/09/13	CEO
Incident Reporting and Managing Procedure	24/11/14	DCA
IG Incident Management SOP	04/03/16	DCA
Acceptable Use Policy	Awaiting approval	BoD
Subject Access Request Procedure	04/03/16	DCA

6. Information Governance Assessment

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 and IT Security
- Informatics
- Medical Records
- Corporate Affairs

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

1. Baseline – 31st July
2. Performance Submission – 31st October
3. Final Submission – 31st March

7. Information Governance Training

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

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

8. Information Governance Framework

Full details of the Information Governance Framework are included in the Information Governance Policy. In addition, in order to fulfil the Information Governance Objectives, the Trust also implements the following:

- The Trust has in place Information Asset Registers and an information risk management process as described above in section 4.2.
- The Trust completes data mapping for flows of personal data.
- All staff are required to comply with Trust policies and procedures, as well as national guidance such as the DoH Code of Practice on Confidentiality
- Confidentiality clauses are included in staff contracts of employment.
- Appropriate data sharing agreements and contractual terms are used with third-parties.
- Staff are made aware of their responsibilities through mandatory IG training
- Implement ‘Privacy by Design’ through the use of Privacy Impact Assessments

Openness

- Non-confidential information on the Trust and its services should be available to the public through a variety of media, in line with the Trust's policy for the FOI(A)
- The Trust will establish and maintain policies to ensure compliance with the FOI(A)
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media
- The Trust will have clear procedures and arrangements for handling queries from patients and the public
- The Trust will include details of any serious untoward incidents associated with information governance within its public Annual Report
- The Trust will provide assurances as to the processes for managing information governance in a sound and robust way within its annual Statement of Internal Control

Legal Compliance

- The Trust regards all identifiable personal information relating to patients as confidential
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- The Trust will establish and maintain policies to ensure compliance with the DPA, Human Rights Act, the Common Law Duty of Confidentiality, the Caldicott Principles and any other relevant law
- 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)

Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources
- The Trust will undertake or commission assessments and audits of its information and IT security arrangements
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Trust will 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

Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records
- The Trust will undertake or commission assessments and audits of its information quality and records management arrangements

- Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training

9. Information Governance Monitoring, Control and Audit

Monitoring Process	Requirements
Who	IG Team
Standards Monitored	IG Toolkit Scores
When	Annually
How	Confirm and Challenge with Internal Audit
Presented to	Information Governance Group
Monitored by	Information Governance Group
Completion/Exception reported to	DCA Governance Group

Monitoring Process	Requirements
Who	IG Team
Standards Monitored	Completion of Specialist Staff Training (TNA at Annex I)
When	Bi-Annually
How	Collection of training certificates from staff
Presented to	Information Governance Group
Monitored by	Information Governance Steering Group
Completion/Exception reported to	DCA Governance Group

Monitoring Process	Requirements
Who	Learning and Development Team
Standards Monitored	95% of Staff Completing Mandatory Information Governance Training
When	Annually
How	Monitoring compliance via ESR
Presented to	Information Governance Group
Monitored by	Information Governance Group
Completion/Exception reported to	DCA Governance Group

Reviewed	4th March 2016
Approved	4th March 2016 – Information Governance Group
Review Date	March 2017

Annex I – Training Needs Analysis

	SIRO	Caldicott Guardian	Information Governance Manager	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 Managament											
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.

Appendix 3

Information Governance Assurance Statement

As of 16th September 2009, all organisations submitting an IG Toolkit assessment are required to accept the following Information Governance Assurance Statement. This happens at the point of submission (i.e. when you click the "Submit" button).

The IG Assurance Statement is binding on your organisation and acceptance should be authorised by an appropriate senior individual in the same way as the IG Toolkit assessment itself. The IG Assurance Statement can be printed (using the "Print" button below) prior to acceptance in order to facilitate consideration by authorising individuals.

Information Governance Assurance Statement for Organisations that use, or plan to use HSCIC Services

Version 4, 10/06/2014

1. All organisations that have either direct or indirect access to HSCIC services[1], including N3, must complete an annual Information Governance Toolkit Assessment and agree to the following additional terms and conditions. Where the Information Governance Toolkit requirements are not met to an appropriate standard (minimum level 2), an action plan for making the necessary improvements must be agreed with the HSCIC External Information Governance team or with an alternative body designated by the Department of Health (e.g. a commissioning organisation).
2. All organisations providing indirect access[2] to HSCIC services for other organisations (approved N3 link recipients), are required to provide the Department of Health, on request, with details of all organisations that have been permitted access, the business justification and the controls applied, and must maintain a local log of organisations to which they have allowed access to N3. This log should be reviewed regularly by the organisation and unnecessary access rights removed. The Department of Health or an alternative body designated by the Department of Health may request sight of these logs in order to facilitate or aid audit or investigations.
3. The approved N3 link recipient is responsible for their compliance with IG policies and procedures and may request authorisation by the Department of Health to monitor and enforce the compliance and conduct of subsidiary connected organisations and suppliers to ensure that all key information governance requirements are met.
4. The use of HSCIC Services should be conducted to support NHS business activities that contribute to the care of patients. Usage of individual services must be conducted inline with those individual services requirements and acceptable use policies. The use of HSCIC provided infrastructure or services for unauthorised advertising or other non-healthcare related activity is expressly forbidden.
5. All threats or security events affecting or potentially affecting the security of HSCIC provided infrastructure or services must be immediately reported via

the HSCIC incident reporting arrangements or via local security incident procedures where applicable.

6. All infrastructure and connections to other systems and networks which are not covered by an approved Information Governance Toolkit Assessment and agreement to this IG Assurance Statement must be segregated or isolated from IGT covered infrastructure and connections such that IGT covered infrastructure and connections, or HSCIC Services are not put at risk. A Logical Connection Architecture diagram must be maintained by network managers in accordance with HSCIC guidance and must be provided for Department of Health review on request.
7. Organisations with access to HSCIC Services shall ensure that they meet the requirements of the Department of Health policy on person identifiable data leaving England, or being viewed from overseas. A copy of the Information Governance Offshore Support Requirements applicable to those accessing HSCIC Services is available on request or can be downloaded from http://systems.hscic.gov.uk/infogov/igsoc/links/index_html. The agreement of the Department to this limited support or exceptionally to more extensive processing must be explicitly obtained.
8. Where another network is connected to N3, only services that have been previously considered and approved by the Department of Health as appropriate for that network are permissible. Requests for new or changed services must be provided to the Department for consideration.
9. Organisations may not create or establish any onward connections to the N3 Network or HSCIC provided services from systems and networks which are not covered by an approved Information Governance Toolkit Assessment and agreement to this IG Assurance Statement.
10. The approved organisation shall allow the Department of Health, or its representatives, to carry out ad-hoc on-site audits, and to review any/all evidence that supports the Information Governance Toolkit Assessment, as necessary to confirm compliance with these terms and conditions and with the standards set out in the Information Governance Toolkit.

Information Governance Assurance Statement

I confirm that I have read, understood and agree to comply with the additional terms and conditions that apply to organisations that have access to HSCIC services and acknowledge that failure to maintain compliance may result in the withdrawal of HSCIC services.

---

[1] HSCIC Services include the N3 network and other applications or services provided by HSCIC, e.g. the NHS Spine Service, NHSmail, Choose and Book (and in future the NHS e-Referral Service).

[2] Access to the N3 network or HSCIC Services via another organisation or gateway