Whittington Health NHS

ITEM: 11/121 **Doc: 10**

Meeting:	**Trust Board**
Date:	**28 September 2011**

Title:	**Information Governance Update**

Executive Summary:	A report on the Information Governance Toolkit assessment and improvement plan for 2011-2012 is presented

Action:	For approval

Report From:	David Emmerson Assistant Director of Information

Sponsor:	Fiona Smith Director of Planning & Programmes (and Senior Information Risk Officer)

Compliance with statute, directions, policy, guidance Lead: All directors	**Reference:** NHS Operating Framework Data Protection Act FoI Act

INTRODUCTION

This report provides an update on the Trust's Information Governance (IG) position with respect to assessments and improvement plans. The formation of Whittington Health in April 2011 meant that responsibility for information governance for the community services transferred however this was not explicitly referenced in the Business Transfer Agreement. Responsibility for IG transferred to the Director of Planning & Performance in June 2011 following completion of the senior management organisational change.

The main NHS-wide mechanism for assessing information governance is the Information Governance Toolkit (IGT). This is a set of requirements specific for a type of NHS organisation. As an acute Trust we have the highest number of requirements; other types of trust such as PCTs, mental health, general practice, and ambulance trusts have a smaller sub-set of requirements.

The list of the 45 requirements applicable to this trust are contained in Appendix 1. 25 of these requirements are designated as "key" and the NHS Operating Framework (Informatics section) places the obligation to achieve Level 2 status for these key requirements in order to be assessed as Satisfactory.

2010-2011 IGT Assessment

A summary report on the 2010-11 assessment is shown below in table 1.

Table 1. 2010-11 IGT Assessment (Number of requirements by Level. Level 3 is the highest rating)

Overall							
Assessment	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Grade**
Version 8 (2010-2011)	0	4	36	5	45	67%	**Not Satisfactory**
Version 7 (2009-2010)	0	0	44	18	62	76%	**GREEN**

Other points to note are:

- The exercise is a self-assessment process.
- The Version 8 requirements for 2010-2011 were very different from the Version 7 requirements in 2009-2010. Although the overall number of requirements was reduced the achievement levels were increased. In addition the evidence requirement to justify the self assessment was made more onerous and demanding.
- The four requirements assessed as Level 1 are all key requirements and the reason for the "Not Satisfactory" rating.
- This is a common pattern of performance across London. At an Information Governance Managers forum in March, only 3 trusts out of 30 represented were declaring a Satisfactory level of compliance. NHS London was not fully compliant.

Islington and Haringey PCTs also made an assessment in 2010-2011 using the IGT although as PCTs they had a different set of requirements. The scores were 90% for Islington and 55% for Haringey.

Current Risks to the 2011-2012 performance

The Trust will be measured against the acute set of indicators and this will now be applied to the whole integrated care organisation. There are a number of current risks to the Trust's information governance assessment:

1. Creation of the ICO and transfer of IG responsibilities

Issue: IG responsibility in the previous PCTs was handled by the commissioning and IT parts of the PCT and did not transfer to the ICO. There has been a loss of "corporate knowledge" about IG issues in the community services and the residual organisations and North Central London have been uncooperative in supplying copies of the 2010-11 PCT IGT assessments.

Mitigation: this issue has been escalated to senior management in NCL to obtain the key information from the previous assessments. Information is needed by the end of October – should there be further delay the matter will be escalated to CEO level.

2. Internal Audit Report

Issue: The internal audit report from Parkhill on the 2010-2011 assessment has not been received and there may be recommendations that must be addressed as part of the 2011-2012 workplan. This audit examined the evidence provided by the Trust and assessed whether it satisfies the IGT standards and uses a methodology prescribed by the Audit Commission.

Mitigation: Parkhill have been requested to provide the outstanding report asap. In the meantime Parkhill have asked for more information and this has provided. The audit report is required by the end of September – if not available then the matter will be escalated to the Director of Finance.

3. Resource implications

Issue: The IG team has had to take responsibility for all IG issues across the acute and both the community services. There is a senior information manager who has handled all IG work for the last two or three years amongst their other duties. The workload could increase significantly as IG queries and work from all parts of the organisation will be sent to the team.

Mitigation: The Information Governance Officer vacant post has now been filled providing additional dedicated resource. Monitoring of workload has started.

Depending on the outcome of the mitigating actions, further consideration will be made in the Autumn on whether add issues to the Trust's risk register.

2011-2012 IG Improvement Plan

The 2011-2012 workplan for information governance is at Appendix 2.

This workplan has been structured around the main IGT initiatives and is a mixture of improvement projects to address particular issues and routine IG work that must be scheduled throughout the year.

There are a number of reporting milestones in 2011-2012.

To	Purpose	Date
Audit Committee	Update on progress against the IG Workplan	December 2012
Trust Board	Update on IG workplan and estimate on 2011-2012 IGT assessment due 31 March 2012	February 2012
IGT Assessment	Full assessment and evidence base uploaded onto the NHS IGT website	31 March 2012

Caldicott Guardian

All organisations are required to have a Caldicott Guardian, a senior clinician with responsibility for protecting the confidentiality of patient information for enabling appropriate information sharing. The Trust's Caldicott Guardian is Dr Maria Barnard who was appointed in late 2011 and whose role has also been extended to community services and is a Trust-wide service.

Freedom of Information

FoI is a separate but linked part of information governance. The FoI Act gave all members of the public the right to obtain non personal information from public organisations, subject to some exemptions.

FoI requests have been managed by the Trust's Corporate Secretary. However following the recent reorganisation this service will transfer to the Director of Strategy from September 2011.

In 2010-2011 the Trust received 201 FoI requests (community service data not available); this is an increase on the 190 in 2009-2010. In the April – July period we have received 73 (expected annual total 219 and this excludes community services requests).

In 2010-2011 61% of FoI requests answered within the 20 day timetable.

The FoI Manager will become a member of the Information Governance Steering Group and a separate FoI workplan will be developed and is expected to address the following issues:

- Re-establishment of the FoI team under the Director of Strategy including a communications plan so all staff are informed
- Integration and monitoring of all FoI requests across the Trust
- Improvements to response times
- Implementation of the FoI Publication Scheme (routine publishing of all standard Trust documentation)

Subject Access Requests under the Data Protection Act

FoI specifically excludes access to patient or other person identifiable data. The Data Protection Act gives individuals the right to have a copy of the information an organisation holds about them and the right to have it corrected where it is wrong.

In 2010-2011 The Whittington Hospital NHS Trust received 1,892 requests from patients, their legal representatives or internally from the Trust Legal Services department. It is expected that the number in 2011-2012 will exceed 2,000.

Community services have a decentralised process for responding to subject access requests, where individual service managers supply the information direct to the requester. Community services have a simpler process with the majority of clinical records on one system (RiO) whereas the hospital data is spread between a number separate clinical and departmental systems. The 2011-2012 workplan at Appendix 2 contains a section to review how subject access requests are managed within a single ICO.

Information Commissioner's Office

The Information Commissioner's Office are the public authority with responsibility for upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Information Commissioner's Office has a range of duties but also have enforcement powers and can fine organisations up to £500,000 for breaches of data protection legislation. Individuals can complain to the Information Commissioner's Office if they consider that an organisation has not complied their request in a timely or complete manner. These complaints can cover both subject access and FoI requests. Where a complaint is made the Information Commissioner's Office will issue a notice to the relevant organisation either requesting more information or requiring the organisation to comply with the request within a set timetable. Complaints that are upheld against an organisation may get used by the Care Quality Commission in the overall Quality & Risk Profile data the produce for each organisation.

In 2010-2011, the Trust received no notices from the Information Commissioner's Office.

Appendix 1

Acute Trust Version 9 (2011-2012)

Requirements List

Req No	Description
Information Governance Management	
9-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda
9-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans
9-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations
9-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation
9-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained
Confidentiality and Data Protection Assurance	
9-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs
9-201	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users
9-202	Personal information 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
9-203	Individuals are informed about the proposed uses of their personal information
9-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data
9-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information
9-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations
9-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines
9-210	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
Information Security Assurance	
9-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs
9-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed
9-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff
9-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority
9-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use

9-305	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
9-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy
9-308	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
9-309	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
9-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error
9-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code
9-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely
9-314	Policy and procedures ensure that mobile computing and teleworking are secure
9-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures
9-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate
Clinical Information Assurance	
9-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience
9-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements
9-402	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care
9-404	A multi-professional audit of clinical records across all specialties has been undertaken
9-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records
Secondary Use Assurance	
9-501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop
9-502	External data quality reports are used for monitoring and improving data quality
9-504	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
9-505	A robust programme of internal and external data quality/clinical coding audit in line with the requirements of the Audit Commission and NHS Connecting for Health is in place
9-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place
9-507	The Completeness and Validity check for data has been completed and passed
9-508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity
9-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national standards

Corporate Information Assurance	
9-601	Documented and implemented procedures are in place for the effective management of corporate records
9-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000
9-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken