







The Royal Wolverhampton Hospitals
NHS Trust

Trust Board Report

Meeting Date:	14th March 2011
Title:	Information Governance Toolkit v8 2010.11 Compliance
Executive Summary:	This report presents the Trust's annual self-assessed level of compliance with the Information Governance Toolkit standards for version 8 2010.11
Action Requested:	The Board is asked to approve the annual submission and note action being taken to ensure the continual improvement towards the standards
Report of:	Director of Finance and Information (SIRO)
Author:	
Contact Details:	Tel 01902 698123 Email kate.collins1@nhs.uk
Resource Implications:	Human resource, IG Officer to deliver training. Time implications for staff to complete online training.
Public or Private: <small>(with reasons if private)</small>	Public Session
References: <small>(eg from/to other committees)</small>	Board Assurance Committee -24th February 2011, Trust Management Team – 4th March 2011
Appendices/ References/ Background Reading	<p>Appendix 1- Final Submission Report 2010/11, by requirement/lead/level</p> <p>Appendix 2 - Version 8 IGToolkit Level 1 Action Plans</p> <p>8-112 Extension news article on the IGToolkit pages https://www.igt.connectingforhealth.nhs.uk/NewsArticle.aspx?tk=406044417343421&Inv=2&cb=b1c2964c-d513-4658-8091-74921bf2a9d1&artid=61&web=yes</p> <p>NHS Operating Framework (Informatics Planning 2010/11). http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_110335</p> <p>Information Governance Toolkit https://www.igt.connectingforhealth.nhs.uk/</p>
NHS Constitution: <small>(How it impacts on any decision-making)</small>	<p>In determining this matter, the Board should have regard to the Core principles contained in the Constitution of:</p> <ul style="list-style-type: none">  Equality of treatment and access to services  High standards of excellence and professionalism  Service user preferences  Cross community working

Background Details

Final Submission V8 IGT 2010.11

A summary of the final levels achieved for Version 8 Final Submission of the IGToolkit can be found in table 1 below and more detail can be found in appendix 1. These scores are to be submit to Connecting for Health via the online Information Governance website by 31st March 2011. The scores are based on evidence collected by requirement leads, assessment and final approval by the requirement leads, review by the IGSG and Medical Director.

Version 8 of the IGToolkit was released July 2010, but required quite a long period of assimilation, since there had been numerous changes to the requirements and a complete change to the online environment provided by the Department of Health (DH) to manage the assessment process. These changes were reported to BAC in October 2010, most noticeable in the Final submission score will be the grading scheme. This has changed, from a RAG system to a Satisfactory/ Unsatisfactory score. A Satisfactory rating will be achieved if all requirements reach a level 2. This change links directly to the NHS Operating Framework (Informatics Planning 2010/11).

The 6 initiatives for information governance are split by the following areas:

- | | |
|--------------------------------------|------------------------------------|
| 1. Information Governance Management | 2. Clinical Information Assurance |
| 3. Confidentiality & Data Protection | 4. Secondary Use Assurance |
| 5. Information Security Assurance | 6. Corporate Information Assurance |

The scores are based on evidence collected by requirement leads, assessment and final approval by the requirement leads, review by the IGSG and Medical Director. Please refer to Appendix 1 for further detail on each initiative, where scores are broken down by topic and lead.

Initiative	Level 0	Level 1	Level 2	Level 3	Not Relevant	Current Score (%)
Information Governance Management	0	1	3	1	0	67%
Confidentiality and Data Protection Assurance	0	0	7	2	0	83%
Information Security Assurance	0	1	8	6	0	78%
Clinical Information Assurance	0	0	5	0	0	67%
Secondary Use Assurance	0	0	3	2	0	75%
Corporate Information Assurance	0	0	3	0	0	67%
All Initiatives	0	2	32	11	0	73%

Overall Assessment

Unsatisfactory. Level 2 or above has not been achieved for every requirement

Action plans

The NHS Operating Framework, Informatics Planning document stipulated that all requirements should be at level 2 by March 2011. However there are 2 areas in our 2010.11 Final Submission which are sitting at a level 1 because the evidence we have did not fundamentally meet the outline for a level 2.

The deadline for requirement 8-112 around training has been extended by Department of Health (DH) until 30th June 2011 the extension outlined in a news article on the IGToolkit pages [here](#). To take advantage of this extension we will submit a statement as such as part of the final submission.

Each requirement which is a level 1 has an action plan to ensure we are actively working on remedial action to ensure an improvement in the scores, we are trying to resolve these issues by the end of March 2011 (June 2011 for training). We ask for delegated permission from the board to alter the declaration if we are confident we can comply with these requirements before the respective deadlines.

Please see appendix 2. The requirements which have scored a level 1 are as follows:

8-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained
8-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate

What this means for the Trust

Implications of level 1's for the Trust may be that:

- The Information Commissioner (ICO) may be interested in our IGToolkit scores to see if we have appropriate procedures to avoid a Data Protection breach. An enforcement notice or fine would be issued for a serious breach or a serious lack of adequate procedures which could lead to a breach.
- The Care Quality Commission quality and risk profiles will reflect our IGToolkit scores, as the Information Governance Toolkit is now used by the CQC to inform risk. The feed through of IGToolkit scores to the risk profile will create a very real and patient focused picture of work to be done and reinforce the significance of our action plans for level 1 requirements.
- We have an internal audit for the first time in early 2011-12, which will evaluate our self assessment and the quality of our evidence. This will give us a strong and accurate standing point to move forward when we go through TCS. However the IGToolkit takes little or no account of structural changes from Transforming Community Services and how these will affect scores. To ensure we have the appropriate assurance and correct evidence after TCS the scores for our IGToolkit return will effectively be 0'ed and built from bottom up when we inherit provider information risks from the PCT.

**Information Governance Toolkit Workbook (Version 8) - Acute Trust
Final Submission Report 2010/11**

IGToolkit uses the following scoring system:

Score	Explanation	
NR	Not relevant to the Trust	
0	Practice does not exist/ is not documented	Lowest score
1	Plans to implement practice are in place	↓
2	Plans are formally approved, process is fully implemented and active	
3	Process is monitored and audited regularly, regular reports to senior level	Highest score

Initiative	Req	Requirement statement	Version 8 Operational Lead	Version 8 Final level
Information Governance Management	8-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Kate Collins	3
	8-105	There are approved and comprehensive IG Policies with associated Strategies and/or improvement plans	Kate Collins	2
	8-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Procurement	2
	8-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	HR	2
	8-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Kate Collins	1
Confidentiality and Data Protection Assurance	8-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	Brian Millar	3
	8-201	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users	Kate Collins, input from HR	2
	8-202	Consent is appropriately sought before personal information is used in ways that do not directly contribute to the delivery of care services and objections to the disclosure of confidential personal information are appropriately respected	Brian Millar/ Kate Collins	2
	8-203	Individuals are informed about the proposed uses of their personal information	Brian Millar/ Chris Wanley/ Kate Collins	2
	8-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Lisa Hughes/ Gail Langston	2
	8-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	Tracey Dunn-Bartlett/ Chris Wanley	3
	8-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Kate Collins	2

	8-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Kate Collins	2
	8-210	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	Chris Wanley/ Nick Bruce	2
Information Security Assurance	8-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Chris Wanley	2
	8-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Chris Wanley	3
	8-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Chris Wanley/Maria Arthur	3
	8-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	Chris Wanley/ Nick Bruce/ HR	2
	8-304	Monitoring and enforcement processes are in place to ensure NHS national application smartcard users comply with the terms and conditions of use	Chris Wanley/ Nick Bruce/ HR	2
	8-305	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	Chris Wanley	2
	8-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	Chris Wanley/ Kate Collins	2
	8-308	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	Malcolm Brown	2
	8-309	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	Malcolm Brown/ Di Preston	2
	8-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Malcolm Brown	3
	8-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	Malcolm Brown	3
	8-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Malcolm Brown	3
	8-314	Policy and procedures ensure that mobile computing and teleworking are secure	Malcolm Brown	3
	8-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Chris Wanley	2
8-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Information/ IT	1	

Clinical Information Assurance	8-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Paul Franklin- Data Quality Kate Collins - Evaluate Corporate Records	2
	8-401	There is consistent and comprehensive use of the NHS number in line with NPSA requirements	Kevin Darcy	2
	8-402	Procedures are in place to ensure the accuracy of service user information on all systems that support the provision of care	Lisa Hughes/ Tracey Dunn Bartlett	2
	8-404	A multi-professional audit of clinical records across all specialties has been undertaken	Kerry Walters/ Scott Adams Lisa Hughes	2
	8-406	Procedures are in place for monitoring the availability of <u>paper</u> care records and tracing missing records	Lisa Hughes	2
Secondary Use Assurance	8-501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	Tracey Dunn- Bartlett	3
	8-502	External data quality reports are used for monitoring and improving data quality	Paul Franklin	2
	8-504	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	Paul Franklin/ John White/ Sian Litkowski	2
	8-505	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	Sian Litkowski	2
	8-506	A documented procedure and a regular audit cycle for accuracy checks on patient data is in place	Paul Franklin/ John White/ David Butterworth	2
	8-507	The Completeness and Validity check for data, as detailed in the guidance document, has been completed and passed.	Paul Franklin/ John White	2
	8-508	Clinical/care staff are involved in validating information derived from the recording of clinical activity	Sian Litkowski	2
	8-510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to National Standards	Sian Litkowski	3
Corporate Information Assurance	8-601	Documented and implemented procedures are in place for the effective management of corporate records	Kate Collins- Evaluate Corporate records	2
	8-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Kate Collins	2
	8-604	As part of the information lifecycle management strategy, an audit of all corporate records has been undertaken	Kate Collins	2

Version 8 IGToolkit Level 1 Action Plans

Req	Requirement statement	V 8 Lead	V 8 level	Requirement	Action plan	Time scale
Information Governance Management						
8-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Kate Collins	1	<p>Level 1:</p> <ul style="list-style-type: none"> - An IG training programme has been developed that includes training needs analyses, induction for new starters and the completion of online basic training using the NHS IG Training Tool. Where necessary, this is supported by local IG induction training and guidance materials. 	<ul style="list-style-type: none"> - Extension of Training deadline by DH to 30th June 2011, Trust will take advantage of the extension. - IG Training to change to an annual requirement in Trust Policy- reported to Ed& Training to update. - Training tool replaced old IG training on KITE site. - IG training site referenced in all online training, Quick induction, Junior doctors induction. - Paper version of training used on mandatory training day - Training being promoted via AUB, KITE Governance Forums. Monthly AUB to be circulated. - Face to face sessions being provided - Computer workshop sessions being provided - Compliance reports, linked to already existing ED& training reports to show departmental compliance. - IG module is already available in OLM- need OLM to be rolled out 	<p>Oct 2010</p> <p>Oct 2010 Jan 2011</p> <p>Oct 2010</p> <p>Ongoing until June 2011 Ongoing Ongoing Ongoing</p> <p>Ongoing 2011</p>
				<p>Level 2:</p> <ul style="list-style-type: none"> - All staff, including new starters, locum, temporary, student and contract staff members have completed (or are in the process of completing) mandated IG training using the NHS IG Training Tool - Staff training needs are assessed to ensure that the basic training provided is sufficient. - Additional training is provided to staff in key roles 	<ul style="list-style-type: none"> - Not compliant until 95% of staff or above have been trained. Continue to promote training via methods outlined in level 1 in order to increase number of staff trained. - TNA to be fed out March 2011, evaluated April 2011. - RISK training resource, currently delivered by IG officer only 0.3 WTE of role, not IG staff being transferred in TCS - RISK TCS will increase the number of staff to be trained and impact on the overall trust percentage. 	<p>Ongoing training</p> <p>Mar 2011</p>
				<p>Level 3:</p> <ul style="list-style-type: none"> - Compliance checks and routine monitoring are undertaken to test staff understanding and to ensure procedures are being complied with. 	<ul style="list-style-type: none"> - RISK not possible with current 0.3 WTE resource 	N/A

Req	Requirement statement	V 8 Lead	V 8 level	Requirement	Action plan	Time scale
Information Security Assurance						
8-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Information/ IT	1	<p>Level 1:</p> <ul style="list-style-type: none"> - Plan for implementing Pseudonymisation, responsible leads.(PIP) 	<ul style="list-style-type: none"> - Plan taken to IGSG on the requirements of project, based on guidance received from Connecting for Health - IT and Information met outside IGAG to discuss issues and a way forward 	<p>Nov 2009</p> <p>Jan 2010</p>
				<p>Level 2:</p> <ul style="list-style-type: none"> - Attain level 2 against all key requirements, of which Req 112(training) is one of them. - Plan business process changes, and a project has been completed documents to support 	<ul style="list-style-type: none"> - Pseudonymisation has not been implemented due to: <ul style="list-style-type: none"> - Lack of central guidance from Connecting for health - No solution centralized from National Programme for IT, means significant piece of work/investment will be needed. - TCS will impact on the systems we have in the Trust and we will need to ensure they are compliant with PIP. Therefore work was not started before TCS. - RISK Cannot reach level 2 because all key req of the IGToolkit must be level 2. Req 112 (training) is a key req and is currently level 1, see above. 	<p>Review March & May 2011 at IGSG</p>
				<p>Level 3:</p> <ul style="list-style-type: none"> - External auditors have reviewed the process of pseudonymisation to ensure that ensure that the business process changes, safe haven processes and technical pseudonymisation and/or anonymisation functionality are working effectively. 	<ul style="list-style-type: none"> - N/A 	<p>N/A</p>