AUDIT YORKSHIRE
The journey to excellence

NHS

Internal Audit Report
For
Leeds and York Partnership NHS Foundation Trust
Information Governance Toolkit
LY14/2018

Contents

Report Author: Surjit Toor
Report Version: Final
Report Date: 26 March 2018

Lead Executive Director: Dawn Hanwell, Chief Financial Officer and Deputy Chief Executive
Lead Officer: Carl Starbuck, Information and Knowledge Manager

Section 1: Executive Summary

Objective

The objective of the review was to gain assurance that the Trusts Information Governance Toolkit (IGT) return is fair and reasonable and that there is sufficient evidence that supports the attainment level for the following sample of 10 requirements reviewed.

Requirement number	Requirement Description
205	Recognising and Responding to a Subject Access Request
206	Confidentiality Audit Procedures
304	NHS Smartcards
311	Prevention and Detection of Malicious and Unauthorised Mobile Code
402	Accurate Collection and Recording of Service User Data
406	Monitoring the Availability of Paper Health/Care Records
501	National Data Definitions, Values and Validation
504	Local and National Benchmarking to Identify Data Quality Issues
506	Effective Audit Cycle for Accuracy Checks on Service User Data
516	Clinical Coding Training

Overall Opinion

Significant	In order to demonstrate compliance with good practice, the Foundation Trust must be able to achieve attainment level 2 on all requirements. The Foundation Trust self-certified as meeting level 2 or above for all IGT requirements. Our testing on a sample of 10 requirements found that sufficient evidence was in place to support a level 2 attainment or above for the 10 requirements.

Section 1: Executive Summary

Assurance on Key Control Objectives

Control Objective	Review Highlights (✓ Positive Assurance, ! Action Required)	Assurance Level	Recommendations (Priority)		
			High	Med	Low
The Information Governance Toolkit return is accurate, complete and scores assigned are appropriate.	✓ On the basis of the 10 requirements tested for this audit, the evidence uploaded or referenced was sufficient to justify the Foundation Trusts self-assessment scores. ✓ The Foundation Trust is expecting to score with a 2 or above in all of the 45 requirements for the March 2018 submission.	Significant	0	0	0
Overall		**Significant**	**0**	**0**	**0**

Background Information

Information Governance relates to the way in which organisations 'process' or handle information. It covers personal information, i.e. that relating to patients/service users and employees, and corporate information, e.g. financial and accounting records.

The Information Governance Toolkit has been developed as a performance tool. It draws together the legal rules and central guidance set out above and presents them as a central set of information governance requirements.

The Toolkit has different information governance requirements for different organisational types. However all organisations have to assess themselves against requirements for:

- Management structures and responsibilities
- Confidentiality and data protection
- Information security

Version 14.1 of the IG Toolkit went live in July 2017. V14.1 is an interim solution pending the introduction of a redesigned toolkit. The new Data Security and Protection Toolkit (DSP Toolkit) was recommended in the National Data Guardian's Review of Data Security, Consent and Opt-outs, and is based around assuring local implementation of the ten data security standards set out in that review.

NHS organisations are required to undertake an assessment at the following stages:

- Baseline and Performance Update 31 October 2017
- Final 31 March 2018

Key Risks

The main risk is that the Trust does not meet the minimum attainment level of 2 against the requirements.

Section 2: Audit Background, Objectives, Scope and Circulation

Objectives & Scope

To provide the Trust with assurance:

- that a Baseline and Performance update has been undertaken and completed.
- that an action plan has been produced where the Trust does not meet level 2 and these have been risk assessed.
- opinion on the validity of the scores based on the available evidence.

Methodology

The objectives of this review were achieved by:

- Reviewing the requirements detailed in Section 1.
- Reviewing the evidence for the requirements.
- Discussions with Information Governance staff

Report Circulation

Draft	Final	Recipient Name	Recipient Title
	✓	Dawn Hanwell	Chief Financial Officer and Deputy Chief Executive
✓	✓	Bill Fawcett	Chief Information Officer
✓	✓	Carl Starbuck	Information & Knowledge Manager Data Protection Officer Freedom of Information Officer Deputy Caldicott Guardian

Acknowledgement

The auditor is grateful for the assistance received from management and staff during the course of this review. The following members of the Audit Yorkshire team were involved in the production of this report:

Head of Internal Audit:	Helen Kemp-Taylor
Audit Manager:	Sharron Blackburn
Project Manager:	Surjit Toor

Date: 27 March 2018

Section 3: Key to Internal Audit Reports

Audit Opinion

The following opinions provide management assurance in line with the following definitions:

Opinion Level	Opinion Definition	Guidance on Consistency
HIGH (STRONG)	High assurance can be given that there is a strong system of internal control which is designed and operating effectively to ensure that the system's objectives are met.	The system is well designed. The controls in the system are clear and the audit has been able to confirm that the system (if followed) would work effectively in practice. There are no significant flaws in the design of the system. Controls are operating effectively and consistently across the whole system. There are likely to be core controls fundamental to the effective operation of the system. A High opinion can only be given when the controls are working well across all core areas of the system. For example with 'Debtors' the controls over identifying income, raising debt, recording debt, managing debt, receiving debt, etc. are all working effectively – there are no serious concerns. Note this does not mean 100% compliance. There could be some minor issues relating to either systems design or operation which need to be addressed (and hence the report may include some recommendations) – however these issues do not have an impact on the overall effectiveness of the control system and the delivery of the system's objectives.
SIGNIFICANT (GOOD)	Significant assurance can be given that there is a good system of internal control which is designed and operating effectively to ensure that the system's objectives are met and that this is operating in the majority of core areas	The system is generally well designed - but there may be weaknesses in the design of the system that need to be addressed. In addition most core system controls are operating effectively – but some may not be. Whilst any weaknesses may be significant they are not thought likely to have a serious impact on the likelihood that the system's overall objectives will be delivered.

Section 3: Key to Internal Audit Reports

LIMITED (IMPROVEMENT REQUIRED)	Limited assurance can be given as whilst some elements of the system of internal control are operating, improvements are required in the system's design and/or operation in core areas to effectively meet the system's objectives	The system is operating in part but there are notable control weaknesses. There are weaknesses in either design or operation of the system that may mean that core system objectives are not achieved. In terms of what differentiates a borderline Significant Opinion to a borderline Limited opinion – the main factors are the scale and potential impact of weaknesses found. Multiple weaknesses across a range of core areas would suggest a Limited Opinion level is applicable. However it also true that ONE weakness can suggest a Limited Opinion if it is fundamental enough to mean that a number of core system objectives will not be achieved.
LOW (WEAK)	Low assurance can be given as there is a weak system of internal control and significant improvement is required in its design and/or operation to effectively meet the system's objectives.	The audit has found that there are serious weaknesses in either design or operation that may mean that the overall system objectives will not be achieved and there are fundamental control weaknesses that need to be addressed. It should be borne in mind that Low Assurance is not 'No Assurance.' The key point here is that there is a good chance that the system may not be capable of delivering what it has been set up to deliver – either through poor systems design or multiple control weaknesses. The report will clearly state if 'No Assurance' is actually more applicable than no assurance.

Where limited or no assurance is given the management of Leeds and York Foundation Trust must consider the impact of this upon their overall assurance framework and their Annual Governance Statement.

Section 3: Key to Internal Audit Reports

Priorities assigned to individual recommendations

Individual recommendations are graded in accordance with the severity of the risk involved to the Foundation Trust. Audit Yorkshire has a standard definition for each level of recommendation priority. This is represented in the table below:

Grading	Definition	Guidance on Consistency
Major (High)	Recommendations which seek to address those findings which could present a significant risk to the organisation with respect to organisation objectives, legal obligations, significant financial loss, reputation/publicity, regulatory/statutory requirements or service/business interruption.	These are recommendations which aim to address issues which if not addressed could cause significant damage or loss to the organisation. The expectation is that these recommendations would need to be taken as a matter of urgency. These recommendations should have a high corporate profile – with a clear implementation tracking process in place, overseen by the Board or a Board level committee.
Moderate (Medium)	Recommendations which seek to address those findings which could present a risk to the effectiveness, efficiency or proper functioning of the system but do not present a significant risk in terms of corporate risk.	These are recommendations which if not addressed could cause problems with the safe or effective operation of the system being reviewed. The recommendations should have appropriate profile within the division or business area in which the system being considered sits and some profile at Board /Audit Committee level also. These recommendations should be carefully tracked to ensure that action reduces the risks found
Minor (Low)	Recommendations which relate to issues which should be addressed for completeness or for improvement purposes rather than to mitigate significant risks to the organisation. (This includes routine/housekeeping issues)	All other recommendations fall into this category. This includes recommendations which further improve an already robust system and housekeeping type issues.

Appendix 1: Controls Evaluation

This matrix sets out the control objectives and expected controls which we expected to see and test as part of this audit.

Where expected controls are either not in place or are not being applied consistently, a recommendation may be raised. Details of all recommended actions to improve controls are given at Section 3.

Recognising and Responding to a Subject Access Request

205	Org. self score	2	Date	03/18	Audit opinion	2	Date	03/18

IG Requirement 205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
1	There is a documented procedure for handling subject access requests that has been approved by senior management or committee.	1a: Responsibility for dealing with subject access requests has been assigned to one or more individuals who have clear procedures to follow.	1a	Named individuals' job description(s) or work area business plans.	• Health Records Manager Job Description. • Information Governance Support Officer Job Description. • Data Protection Act (1998) Subject Access Request Procedure.	Satisfactory.
		1b: There is a documented procedure for processing subject access requests efficiently and in accordance with the law.	1b	Documented procedure for processing subject access requests which includes the details of the named staff member(s), job role(s) or responsible group.	• Data Protection Act (1998) Subject Access Request Procedure. • Application for access to health records.	Satisfactory.
		1c: The procedure has been approved by senior management, an appropriate committee or other established local governance process.	1c	Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriately senior manager.	• Minutes of the Information Governance Group (IGG) where the Data Protection Act (1998) Subject Access Request Procedure was approved.	Satisfactory.

2	Subject access requests are actioned by fully trained and resourced staff and all staff members are aware of the need to support subject access requests, and where in the organisation such requests should be directed. The procedure has been implemented effectively to meet the statutory deadlines.	2a: All staff assigned responsibility for processing subject access requests have been appropriately resourced and trained to do so.	**As level 1 plus:**			
			2a	Minutes of meetings, in a document or email outlining the allocation of appropriate resource to process subject access requests (e.g. time, budget, managerial support, etc).	• Subject access processing performance report presented to IG Group. April, May, July 2017. • Minutes of the Information Governance Group (IGG) April, May, July 2017 • DPA-SAR logging spreadsheet, which has maintained a record of performance on medical records SARs since August 2015.	Satisfactory.
			2a	Training needs analysis forms, training attendance lists, staff briefing materials covering how to manage a subject access request, presentations, or training evaluation records.	• Health Records Team HSCIC IG Training Tool – SAR Training Compliance.	Satisfactory.
		2b: All staff members are aware of their responsibility to support subject access requests and where in the organisation such requests are ultimately handled. Front-line staff members are provided with more detailed guidance about the procedure to follow. Staff might be informed through team meetings, awareness sessions, staff briefings, or staff may be provided with their own copy of the procedure.	2b	Agendas, notes, minutes, briefing materials or in the case of personal copies being provided to staff, a list of signatures that they have read and understood the procedure.	• Data Protection Act (1998) Subject Access Request Procedure, is available on Staff net and is available to all staff. • Trust wide e-mail sent to all staff informing them of the procedure.	Satisfactory.

		2c: The subject access procedure has been effectively implemented, which means that requests are appropriately recognised, timescales are met and appropriate information is provided.	2c	A documented review of the subject access requests received.	• Subject access processing performance report presented to IG Group. April, May, July 2017.	Satisfactory.

Appendix 1: Controls Evaluation

AUDIT YORKSHIRE
The journey to excellence

Confidentiality Audit Procedures

IG Requirement 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.**

206	Org. self score	3	Date	03/18	Audit opinion	3	Date	03/18

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
1	There are documented confidentiality audit procedures in place that include the assignment of responsibility for monitoring and auditing access to confidential personal information. The procedures have been approved by senior management or committee and have been made available throughout the organisation.	**1a:** Responsibility for documenting confidentiality audit procedures that cover monitoring and auditing access to confidential personal information has been assigned to an individual or group. **1b:** There are documented confidentiality audit procedures that clearly set out responsibilities for monitoring and auditing access to confidential personal information. **1c:** The procedures have been approved by senior management, an appropriate committee or other established local governance process and have been made available	1a	A named individual's job description, a note or e-mail assigning responsibility or the terms of reference of a group.	• Terms of Reference of the Information Governance Group who have responsibility. • Minutes of the Information Governance Steering Group.	Satisfactory.
			1b	Documented confidentiality audit procedures which include the details of the named staff member, job role or responsible group.	• PARIS Confidentiality Audit Procedures. (IG Team local procedure note) • Terms of Reference of the Information Governance Group who have responsibility. • NHS Spine Alert Confidentiality Audit Procedures (IG Team local procedure note)	Satisfactory.
			1c	Approval/sign off within the minutes of meetings, in a document or email or a personal endorsement in writing from an appropriately senior manager.	• NHS Spine Alert Confidentiality Audit Procedures. (IG Team local procedure note) • PARIS Confidentiality Audit Procedures. (IG Team local procedure note)	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
		throughout the organisation.			• Minutes of the Information Governance Steering Group approving the Confidentiality Audit Procedures and	
			1c	Inclusion in a staff handbook, or publishing the procedures on the Intranet or personal copies of the procedures provided to staff (in the latter case there may be a list of staff signatures confirming receipt of the procedures) or the evidence may be a description of the dissemination process or minutes of the meeting where the process was decided.	• IG presentation slides. • Note: although the existence of functionality and audit is presented at induction, the methodology and procedure is not publicised, as this may compromise security by illustrating how we audit.	Satisfactory.
2	All staff members with the potential to access confidential personal information have been made aware of the procedures. The procedures have been implemented and appropriate action is taken where confidentiality processes have been breached.	**2a:** All staff members with the potential to access confidential personal information have been informed that monitoring and auditing of access is being carried out, of the need for compliance with confidentiality and security procedures and the sanctions for failure to comply. Staff might be informed through team meetings, awareness sessions, staff briefing materials, or staff may be provided with their own copy of the procedures.	**As level 1 plus:**			
			2a	Minutes/notes of meetings, briefing and awareness session materials or a list of staff signatures that they have read, understood and will comply with the procedures.	• IG presentation slides. • Screen shot of message for all PARIS users, making then aware of code of conduct in respect of confidentiality.	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
		2b: The procedures have been effectively implemented and appropriate action is taken where confidentiality processes have been breached or where a near-miss has occurred. Therefore staff compliance is monitored and there are case reviews if confidentiality processes have been breached or if there has been a near-miss incident.	2b	Completed monitoring form, or a report on the outcome of staff compliance checks.	• Screen shot of IG Group incident reporting spreadsheet.	Satisfactory.
			2b	Where a breach has occurred, copies of Serious Incidents Requiring Investigation reports, lessons learned reports, staff feedback briefings, staff retraining files, or disciplinary documents. Evidence may also be found in public statements and communications to service users.	• Note: An "on request" audit has been carried out relating to the Leeds Teaching Hospitals e-Results service. As this is a system that the Trust does not host, audit is undertaken on our behalf by LTHT colleagues. Outcomes as follows:-Staff initials WD:- audit requested by Sharon Haskins / Alison Stubley – investigation currently ongoing under Zoe Stott's lead. Allegation that a member of staff with access to the LTHT lab results server had inappropriately accessed the system to find results of 2 colleagues. Carl Starbuck has the e-mail trail on file for scrutiny if required.	Satisfactory.
			2b	Where a near-miss has occurred, copies of near-miss reports, lessons learned reports, staff feedback briefings, staff retraining files, or disciplinary documents.	• Note: An "on request" audit has been carried out relating to the Leeds Teaching Hospitals e-Results service. As this is a system that the Trust does not host, audit is undertaken on our behalf by LTHT colleagues. Outcomes as follows:- Staff initials WD:- audit requested by Sharon Haskins	Satisfactory.

Appendix 1: Controls Evaluation

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
					/ Alison Stubley – investigation currently ongoing under Zoe Stott's lead. Allegation that a member of staff with access to the LTHT lab results server had inappropriately accessed the system to find results of 2 colleagues. Carl Starbuck has the e-mail trail on file for scrutiny if required.	
3	Access to confidential personal information is regularly reviewed and there are comprehensive audit trails that detail when confidential personal information has been accessed. Where necessary, measures are put in place to reduce or eliminate frequently encountered confidentiality events.	3a: Access to confidential personal information is subject to regular review and, where necessary, measures are put in place to reduce or eliminate frequently encountered confidentiality events. 3b: All systems holding confidential personal information have audit trails that detail anyone and everyone that has accessed a record.	3a	Minutes/ meeting notes where access has been reviewed during the year including the decisions made such as new guidance for staff, improved physical security measures, documented IT system changes (e.g. stronger password formation; port control to prevent download of personal information to USB sticks, etc) or other new processes.	• Minutes of the IGG May 2017. • Minutes of the IGG April 2017.	Satisfactory.
			3b	Audit trails and system logs.	• NHS Spine Alert Confidentiality Audit Procedures. Screen shot of system log. • PARIS Confidentiality Audit Procedures. Screen shot of system log.	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
		3c:[Only required if Attainment Level 3 was achieved in any previous assessment. Please note that these details will NOT be automatically rolled over and must be completed separately each year.]Policy and law change over time as do technological developments and it is important that the content of procedures is regularly reviewed, is aligned with the latest central guidelines and takes into account any new systems or processes introduced into the organisation.	3c	Minutes/meeting notes where the procedures have been reviewed during the year including the decisions made and any updates to the procedures.	• Minutes of the IGG May 2017. • Minutes of the IGG April 2017.	Satisfactory.

NHS Smartcards

IG Requirement 304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use.

304	Org. self score	2	Date	03/18	Audit opinion	2	Date	03/18

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
1	A plan has been developed for ensuring compliance with the terms and conditions of Smartcard usage, which includes procedures for monitoring and enforcing compliance. The plan has been agreed by senior management or committee.	**1a-** Responsibility has been assigned for developing a plan to monitor and enforce user compliance in regard to Smartcard usage. **1b-** The plan/procedure identifies how users will be informed of their NHS Smartcard usage responsibilities and how compliance will be monitored. There should be clearly defined actions linked with Human Resource processes for dealing with breaches in the NHS Smartcard usage. **1c-** The plan and associated procedures have been approved by senior management, an appropriate committee or other established local governance	1a	A named individual's job description, a note or e-mail assigning responsibility or the terms of reference of a group.	• Information Governance Policy. • Registration Authority Manager Job Description and responsibilities. • Letter from RA to Chief Executive confirming RA responsibilities.	Satisfactory.
			1b	Plan/procedure identifies how users will be informed of their NHS Smartcard usage responsibilities.	• Recruitment and Selection Procedure. The Trusts HR and RA processes are integrated - both utilising the (ESR). • Disciplinary Procedure. • RA terms and conditions document.	Satisfactory.
			1b	Documented audits of compliance.	• NHS Spine Alert Confidentiality Audit Procedures. This is undertaken by Carl Starbuck.	Satisfactory.
			1c	Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriate senior manager.	• Letter from RA to Chief Executive confirming RA responsibilities. • Note: RA implementation was undertaken in line with National RA requirements	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
		process.			and therefore dictated by national policy as set by HSCIC.	
			1c	RA Plan/procedure.	• Recruitment and Selection Procedure. The Trusts HR and RA processes are integrated - both utilising the (ESR). • Disciplinary Procedure. • RA terms and conditions document.	Satisfactory.
2	The plan and procedures have been implemented and all Smartcard users have been effectively informed that Smartcard usage will be monitored and of the need for compliance and the sanctions for non-compliance.	**2a-** The procedures for dealing with breaches in Smartcard usage are accessible to users.	**As level 1 plus:**			
			2a	Procedures included in a staff handbook or published on the Intranet, or within a procedure folder on the network.	• Recruitment and Selection Procedure. The Trusts HR and RA processes are integrated - both utilising the (ESR). • Disciplinary Procedure. • RA terms and conditions document.	Satisfactory.
		2b- The plan has been implemented and all Smartcard users including new, temporary and contract staff members are aware that compliance with the terms and conditions of smartcard usage is monitored and of the procedures for breach and disciplinary measures.	2b	Staff briefing and induction materials.	• Power point presentation on IG detailing staff responsibilities.	Satisfactory.
			2b	Documented audits showing processes for monitoring NHS Smartcard usage and compliance with the NHS Smartcard terms and conditions.	• Spine Alert Tracker – Challenged Alerts. • Screen shot of audit report on the Care Identity Service on 05/03/2018.	Satisfactory.
			2b	Audit report on the outcome of checking that all NHS Smartcard users have electronically signed their terms and conditions.	• Spine Alert Tracker – Resolved Investigation Examples.	Satisfactory.

Prevention and Detection of Malicious and Unauthorised Mobile Code

IG Requirement 311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code

311	Org. self score	2	Date	03/18	Audit opinion	2	Date	03/18

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
1	All Information Assets have been reviewed to identify those which are vulnerable to malicious or mobile code and appropriate controls and procedures have been identified and documented to enable the rapid detection, isolation and removal of malicious code and unauthorised mobile code.	1a: All Information Assets have been identified.	1a	Documented Information Asset Register.	• Asset Register of of PCs'. • Note: The Trust takes the stance that all systems have the potential to hold patient identifiable data and are at risk of being effected by malicious code therefore ALL information assets are logged and monitored.	Satisfactory.
		1b: There are appropriate controls and procedures in place to protect against malicious code and unauthorised mobile code for each of the identified information assets. IAOs have established policy and plans for system patching that takes account of known product support expiry.	1b	Documented controls and procedures for the protection against malicious code / weakness exploitation and unauthorised mobile code for each information asset.	• Standard build document used for Dell PC's. • Cyber security screen shots communicated via staff net. • Failed attempts spreadsheet. • Email Use Policy. • Internet Use Policy. • Encryption Policy. • Network Security Policy. • Note: Sophos Endpoint Security and Control has been deployed on all Trust's PCs, laptops and servers. This is controlled and managed centrally. • CareCERT Cyber Threat Log •	Satisfactory.

Appendix 1: Controls Evaluation

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
2	The approved and documented controls and procedures to mitigate against malware risks have been implemented.	2a: The documented controls and procedures are fully implemented across the organisation.	**As level 1 plus:**			
			2a	Reports generated by the anti-virus/malware solution.	• Minutes of meeting December 2017. Cyber Security is now a standing agenda item at IG Group meetings. • Screen shot of PC. Sophos Endpoint Security and Control has been deployed on all Trust's PCs, laptops and servers. • Note: When ICT are aware of any issues, for example, when they are notified that malicious emails are in circulation - they advise staff via Staffnet	Satisfactory.
		2b: All new Information Assets or changes to existing assets are considered and approved by an appropriate accountable individual (e.g. the IAO or their nominated Information Asset Administrator) to ensure that all risks are adequately managed including the risks relating to malicious or mobile code.	2b	A documented policy or procedures.	• The ITIL aligned Change and Release documentation.	Satisfactory.
			2b	Where new assets have been introduced or changes made, evidence of compliance with the policy/procedure may be in risk analysis documents or in the minutes of meetings. (See also requirement 210)	• Minutes of Senior Management Meeting 22nd August 2016. • Terms of Reference Information Strategy Steering Group. • Minutes of Information Strategy Steering Group.	Satisfactory.

Accurate Collection and Recording of Service User Data

IG Requirement 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.

402	Org. self score	2	Date	03/18	Audit opinion	2	Date	03/18

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
1	There are documented and approved procedures to ensure the accuracy of service user information on all systems and/or records that support the provision of care.	**1a-** Responsibility has been assigned to an individual or group to develop and implement procedures for ensuring the accuracy of service user information on all systems and/or records that support the provision of care.	1a	A named individual's job description, a note or e-mail assigning responsibility or in the terms of reference of a group.	• Terms of Reference of the Performance, Information and Data Quality Group(PIDQG) • Minutes of the Care Services Strategic Management Group, where the TOR for the PIDQG were approved.	Satisfactory.
		1b- The procedures have been documented.	1b	One or more documented procedures (an overall data quality procedure incorporating best methods of checking information with service user, reporting errors and omissions with data, dealing with duplicate registrations/records and reconciling databases).	• Data Quality Policy. • PARIS Data Collection and Input Procedure. Next review date: 27th July 2018	Satisfactory.
		1c- The procedures have been approved by a responsible senior manager, senior management or committee.	1c	Minutes of meetings, in a document or email, or a personal endorsement in writing from an appropriately senior manager.	• Minutes of the Finance & Business Committee Meeting approving the PARIS Data Collection and Input Procedure. • Minutes of the IGG advisory Group approving the Data Quality Policy.	Satisfactory.

Appendix 1: Controls Evaluation

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
2	Data collection and validation activities are regularly monitored. All staff collecting and recording data are effectively trained to do so and dedicated staff take appropriate action where errors and omissions are identified.		**As level 1 plus:**			
		2a- Data collection and validation activities are regularly monitored and data quality reports routinely considered by senior management or data quality committee.	2a	Documented data quality reports (refer to paragraph 29 of the guidance for further detail).	• Note: Virtually all information in our electronic patient information system can be drilled-down to individual staff or patient detail. Reports can be developed as and when requested. • Inpatient Completeness & Validity check report. • Trust Data Completeness Report. • Data quality screen shots evidence document. • Data quality report presented to the Board.	Satisfactory.
		2b- Procedures have been made accessible to all staff involved in data collection activities.	2b	A list of staff signatures confirming that they have read and understood the procedures.	• PARIS Data Collection and Input Procedure. • Data Quality Policy. • Information Governance Policy. • Procedure for the Collection and Input of Service User Information	Satisfactory.
		2c- All staff entering data are effectively trained to accurately collect and record service user information, check the information with an appropriate source and report errors or omissions.	2c	Training materials, training attendance records, or staff briefings.	• Paris Training Booking Guide. • Note: All staff entering data on the PARIS system are trained PRIOR to accessing the PARIS system and are granted 'role based access' depending on their responsibilities / job.	Satisfactory.
			2c	Errors/omission logs.	• Note: All staff are responsible for ensuring that the data they enter into PARIS is of good	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
					quality. The responsibility to correct any errors rests with the local service or clinician. Staff must ensure that they comply with legislation and local Trust policies and procedures. This is incorporated into job descriptions. Persistent failure to comply with these policies and procedures may lead to staff being referred under the Disciplinary Procedure.	
		2d- Dedicated staff carry out activity reconciliations between the service user record and data held on systems that support the provision of care and correct errors and omissions.	2d	Job descriptions of dedicated staff who carry out activity reconciliations.	• Data Quality Co-ordinator (Analyst) Job Description. • Minutes of the Care Services Performance, Information and Data Quality Group Meeting.	Satisfactory.
			2d	Audit or system reports showing that the databases have been synchronised, system reports showing errors/omissions have been corrected, or regular data quality reports.	• Note: Virtually all information in our electronic patient information system can be drilled-down to individual staff or patient detail. Reports can be developed as and when requested. This is achieved by, for example, confirming caseload lists and activity levels through reporting which may also be used for Consultant appraisals. • Screen shot of validation checks.	Satisfactory.

Confidentiality Audit Procedures

IG Requirement 406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records

406	Org. self score	3	Date	03/18	Audit opinion	3	Date	03/18

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
1	There are documented and approved procedures to monitor the availability of paper health/care records, including tracking records and tracing missing records.	**1a:** There are documented procedures in place for monitoring paper health/care record availability, which includes measures to track records removed from the records storage area, to take appropriate action when records are unavailable and to trace missing records.	1a	One or more written procedures including clear guidance for staff and a process to report unavailable or missing records.	• Health Records Policy. • The Management of Incidents Including Serious Incidents Procedure	Satisfactory.
		1b: The procedures have been approved by senior management, an appropriate committee or other established local governance process.	1b	Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriately senior manager.	• Development of Procedural Documents Procedure. • Health Records Policy, detail ratifying committee. • The Management of Incidents Including Serious Incidents Procedure detail ratifying committee.	Satisfactory.
2	The procedures for monitoring the availability of paper health/care records have been implemented and action taken where availability of records is considered poor.	**2a:** All relevant staff members have been informed about the procedures, and in particular of their own responsibilities to comply with the record tracking process, and to	**As level 1 plus:**			
			2a	Minutes/meeting notes of team meetings, briefing materials used in awareness sessions or training materials.	• Health Records Policy. • Note: Health records policy available on the Trust intranet and advertised via trust wide communications at re-launch.	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
		appropriately report unavailable or missing records. Informing staff may be through team meetings, awareness sessions, staff briefings or training (e.g. on induction or in specific training programmes). **2b:** The procedures have been effectively implemented and appropriate reports are provided to senior management, an appropriate committee or other established local governance process. Actions are taken where availability of paper health/care records is poor.			• Screen shot of advertising campaign undertaken by the Health Records Manager	
			2b	Tracking and tracing logs, completed availability monitoring forms, incident reports, key performance indicator (KPI) reports (which may include missing records KPIs, records tracked to certain locations, records not received) and documented evidence of any actions taken.	• DATIX extracts – Missing Records Incidents – 2017-2018 paper. • Screen shot - Medical Records – files requested / found monthly returns.	Satisfactory.
			2b	Documented reports to, or within minutes of meetings of senior management, appropriate committee or other established governance process.	• Note: Reporting of incidents via the usual DATIX mechanism.	Satisfactory.
3	Staff compliance checks are routinely undertaken to ensure staff are following the record tracking process and appropriately reporting unavailable or missing records.	3a: Providing staff with briefing materials and awareness sessions does not provide sufficient assurance that procedures have been understood and are being followed, therefore compliance spot checks and routine monitoring are conducted.	3a	Completed monitoring forms, or a report on the outcome of staff compliance checks.	• DATIX extracts – Missing Records Incidents – 2017-2018 paper. • Screen shot - Medical Records – files requested / found monthly returns. • Note: E-mails from Medical Records document the routine monitoring of successful tracing actions for records pulled from storage for clinics, and any incidence of failed tracing.	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
		3b: [Only required if Attainment Level 3 was achieved in any previous assessment. Please note that these details will NOT be automatically rolled over and must be completed separately each year.]It is important that the procedures are regularly reviewed and updated to ensure that they are aligned with the latest central guidance.	3b	Minutes/meeting notes where the procedures have been reviewed during the year including the decisions made and any updates to the procedures.	• DATIX extracts – Missing Records Incidents – 2017-2018 paper. • Screen shot - Medical Records – files requested / found monthly returns. • Note: Overall the level of unavailable records – 3 instances in the financial year to date – remains negligible and not in need of large scale review.	Satisfactory.

National Data Definitions, Values and Validation

IG Requirement 501	National data definitions, standards, values and data quality checks are incorporated within key systems and local documentation is updated as standards develop							
501	**Org. self score**	2	**Date**	03/18	**Audit opinion**	2	**Date**	03/18

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
1	All key service user information systems incorporate national NHS and/or care definitions and values.	**1a:** Responsibility for ensuring that key service user information systems and documentation for local systems are kept up-to-date in the light of developing national guidance and standard definitions has been assigned.	1a	A named individual's job description, an email assigning responsibility, or terms of reference of a group.	• Data Quality Analyst Job Description.	Satisfactory.
		1b: Key service user information systems incorporate national definitions and values.	1b	A system design document or in outputs from the system for example showing that information is held in standard format and health/care episodes are appropriately coded.	• Screen shot of mandatory fields that have to be completed. PARIS) has fields 'Mandated' to ensure that national definitions and values are captured. • Screen shot of Trust wide Communications (May 2017) about the capturing of patient data on PARIS. • Clinical Coding report November 2017.	Satisfactory.
2	Service user information systems have data quality checks built in that cannot be switched off or be overridden by operational staff. All documentation for	**2a:** Data quality checks have been built into the systems and they cannot be switched off or overridden by operational staff.	**As level 1 plus:**			
			2a	Utilities, procedures, system documentation or system configuration details.	• Data Quality Audit Inpatient / Outpatient Dataset Consistency. • Clinical Coding report November 2017.	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & file ref.	Audit Opinion
	key service user information systems is regularly reviewed and updated in line with changes to national NHS and/or care standards definitions and values.	**2b:** All documentation for local systems is regularly reviewed and updated in line with changes to national NHS and/or care standards definitions and values.	2b	Review documents, minutes of review meetings, follow up actions resulting from review findings and updates to documentation.	• Link to the Trust Integrated Quality and Performance Report (IQPR), which is produced every month and on the third month (March, June, September, December) a quarterly view is included covering the previous three months. This quarterly view includes additional information and an additional set of indicators for us to measure our quality and performance against. • Paris Procedure and via 'easy read' document. Email sent to all staff about the procedure to ensure information is input in line with the Accessible Information Standard. • Sexual Orientation monitoring document. Email sent to all staff about the ISN, which must be implemented by 31/03/2019. • Trust wide email communication informing staff about 'recording ethnicity' in the Paris system.	Satisfactory.

Local and national benchmarking to identify data quality issues

IG Requirement 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.

504	Org. self score	2	Date	03/18	Audit opinion	2	Date	03/18

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
1	Documented procedures have been developed for using local and national benchmarking to identify possible data quality issues and analyse data quality trends over time.	**1a:** The sources of local and national benchmarking have been identified.	1a	Link to source of benchmarks, website link, extract from published document.	• Clinical Coding report November 2017. • Link to the Trust Integrated Quality and Performance Report (IQPR), which is produced every month and on the third month (March, June, September, December) a quarterly view is included covering the previous three months. This quarterly view includes additional information and an additional set of indicators for us to measure our quality and performance against.	Satisfactory.
		1b: There are documented procedures with clearly assigned accountable owners, for using local and national benchmarking to identify possible data quality issues including analysing trends in information over time and	1b	Documented procedures for local and national benchmarking, which references responsibility/accountability for the implementation of the procedure.	• The National Bench-marking Process document. • National Quarterly Submission step by step guide.	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
		making comparisons between periods. **1c:** The procedures have been approved by senior management, an appropriate committee or other established local governance process.			• Burst Out reports to Service Managers.	
			1b	Job description showing assigned responsibility for data quality analysis.	• Data Quality Analyst Job Description. • Performance and data quality manager Job Description.	Satisfactory.
			1c	Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriately senior manager.	• Terms of reference of the Performance, Information and Data Quality Group. • Minutes of the Performance, Information and Data Quality Group. • National Bench-marking Process document.	Satisfactory.
2	The procedures have been appropriately implemented, and local and national benchmarking is used to identify and investigate data quality issues and analyse data quality trends over time.	**2a:** Staff members with the appropriate capability and capacity have been assigned the responsibility of analysing and investigating data quality issues. **2b:** The procedures have been implemented and local and national benchmarking is used to identify possible data quality issues. Where unexpected variation is identified it is investigated through local dialogue and basic checks.	2a	Job description AND a work plan, a formal task list, a work package or an email.	• Data Quality Analyst Job Description. • Screen shot of MHSDS validation reporting.	Satisfactory.
			2b	Review reports of local and national benchmarking data.	• Minutes of the Performance Information and Data Quality Group where National Reporting has been discussed (Chaired by our Chief Information Officer and attended by Lynn Parkinson our Deputy Operating Officer).	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
					• NHS Benchmarking Network Inpatient and Community Mental Health Benchmarking report. • Mental Health Toolkit 16/17. • Mhsds record count excel document Jan 2018.	
			2b	Documented action plans developed as a result of the findings of local and national benchmarking.	• Caseload management dashboard. • Report to Board. • Quality Report 2016/17'	Satisfactory.
			2b	Reports on the outcomes of meetings/discussions with staff and the outcomes of checks of data entry practices.	• Minutes of the Performance Information and Data Quality Group where National Reporting has been discussed (Chaired by our Chief Information Officer and attended by Lynn Parkinson our Deputy Operating Officer).	Satisfactory.
		2c: Trends in data quality are analysed over time, and unexpected variations are investigated and where appropriate, corrected before official submission of data or returns.	2c	Analysis reports, output documentation showing corrected data.	• Validation reporting checks.	Satisfactory.
			2c	Documented action plans developed as a result of trend analysis.	• Screen shot of sign off process which states that the service managers receive an email and that there is a 2 week period for validation and review.	Satisfactory.

Effective Audit Cycle for Accuracy Checks on Service User Data

IG Requirement 506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place

506	Org. self score	2	Date	03/18	Audit opinion	2	Date	03/18

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
1	Data quality is addressed as part of the Information Lifecycle Management Policy and a documented procedure and a regular audit cycle for accuracy checks on service user data is in place.	**1a:** Responsibility for developing the policy and an audit plan for checking the accuracy of service user data has been assigned to the data quality review/monitoring group. **1b:** There is a documented and approved audit plan that includes service user data accuracy audits. **1c:** Staff guidance on accuracy checking has been publicised and distributed to easily accessible locations targeting all relevant staff.	1a	A note or e-mail assigning responsibility or the terms of reference of a group.	• Performance and data quality manager job description. • Data Quality Policy. • PARIS Data Collection and Input Procedure.	Satisfactory.
			1b	A documented audit plan that includes service user data accuracy audits.	• Data Quality Audit Inpatient / Outpatient Dataset Consistency document.	Satisfactory.
			1b	Minutes of the meeting where the audit plan was approved or email or personal endorsement in writing from an appropriate senior manager.	• Minutes of the Information Governance Standing Support Group detail approval of the above document.	Satisfactory.
			1c	Staff guidance published on the intranet, or hard copies found in staff communal areas or in departmental procedures folders.	• Data Quality Compliance Audit of the Input of Data into Trust Systems February 2018. • Data Quality Policy • Information Governance Policy	Satisfactory.

Appendix 1: Controls Evaluation

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
2	The accuracy of service user data audits cover all key data items identified in the supporting guidance for this requirement. The results are documented and reported to the Board/senior management, or delegated sub-committee as part of ongoing data quality progress reviews and made available to the HSCIC if requested.	**2a:** The accuracy of service user data audits, conducted in accordance with the guidance provided and sample sizes specified in the supporting document for this requirement, covers all key data items.	2a	Methodology documentation, audit working papers (for example working papers should include a completed template example of how data accuracy is checked, which includes all required key data items).	• Inpatient Completeness & Validity check report. • Trust Data Completeness Report. • Data quality screen shots evidence document. • Data quality report presented to the Board. • Procedure for the Collection and Input of Service User Information'	Satisfactory.
		2b: Audit reports are documented, with recommendations and agreed actions for improving poor accuracy.	2b	Copy of audit report and recommended actions.	• Internal audit report on data quality. February 2016. • Internal audit report on data quality June 2017.	Satisfactory.
		2c: Progress updates are reported to the Board, delegated sub-group or senior management at set intervals.	2c	Minutes of the meeting where the audit reports were reviewed.	• Minutes of the Performance, Information and Data Quality Group.	Satisfactory.

Clinical Coding Training

IG Requirement 516	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards

516	Org. self score	2	Date	03/18	Audit opinion	2	Date	03/18

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
1	There is a programme of clinical coding mental health training conforming to national standards for all clinical coding staff entering coded clinical information.	**1a:** All clinical coding staff (who assign ICD-10 and OPCS-4 codes), and mental health clinicians who undertake some clinical coding, receive training conforming to national standards (see paragraphs 3-6 of the guidance to this requirement for further details on training requirements).	1a	A departmental training plan document or a copy of the attendee's course certificate of successful completion and proof of the employee's start date of employment as a clinical coder. For clinicians the evidence should be a copy of the course certificate of successful completion.	• Note: The Trust Electronic Staff Records (ESR) system holds training information records for Carol Cook – Clinical Coding Officer. Jayne Hardcastle – Medical Records Officer / Clinical Coding Officer. • Training spreadsheet of Carol Cook.	Satisfactory.
			1a	Copies of any anonymised completed action plans as required during the course.	• Clinical Coding training assessment document for Carol Cook and Jayne Hardcastle.	Satisfactory.
		1b: The mental health clinical coding course is delivered by a Clinical Classifications Service approved clinical coding trainer using only materials endorsed by the Clinical Classifications Service or developed in accordance with national clinical coding standards.	1b	A copy of the attendee's course certificate of successful completion. Confirmation of approved clinical coding trainer status can be obtained by emailing information.standards@hscic.gov.uk.	• Training certificates for both Coders having undertaken refresher training.	Satisfactory.
			1b	Email from the Clinical	• Screen shot of email	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
				Classifications Service confirming proof of clinical coding trainer's 'approved' status.	from the clinical coding trainers.	
2	A programme of mental health clinical coding standards refresher, or four-day clinical coding standards refresher course training every three years for all clinical coding staff entering coded clinical information is in place that conforms to national clinical coding standards. Where appropriate, clinical coding staff have attended specialty and update training workshops when classification revisions require.	**2a:** All clinical coding staff (who assign ICD-10 and OPCS-4 codes) and mental health clinicians who undertake some clinical coding, attend a mental health clinical coding standards refresher or a four-day clinical coding standards refresher course (see paragraph 7 of the guidance to this requirement for further details on refresher training requirements).	2a	A departmental training plan document or a copy of the attendee's refresher course certificate of successful completion and proof of attendance on any previous refresher training courses. For clinicians, the evidence should be a copy of the refresher course certificate of successful completion.	• Training certificates for both Coders having undertaken refresher training.	Satisfactory.
			2a	Copies of any available certificate / screen prints from the mandatory eLearning package (only if attendance is on a four-day Clinical Coding Standards Refresher Course instead).	• Clinical Coding training assessment document for Carol Cook and Jayne Hardcastle.	Satisfactory.
			2a	Copies of any anonymised completed action plans as required during the course.	• Clinical Coding training assessment document for Carol Cook and Jayne Hardcastle.	Satisfactory.
		2b: Clinical coding staff and clinicians who assign ICD-10 and OPCS-4 codes within the organisation attend, where appropriate, clinical coding specialty and update training workshops when classification revisions require.	2b	A copy of the attendee's specialty and update workshop certificate of successful completion / attendance and proof of attendance on any previous update training courses. For clinicians, the evidence should be a copy of	• Clinical Coding training assessment document for Carol Cook and Jayne Hardcastle. • To support the latest coding standards, the Trust procures coding	Satisfactory.

Level	Criterion	Assurance Required		Sources of Assurance/ Evidence	Evidence obtained & File ref.	Audit Opinion
				the specialty and update workshop certificate of successful completion / attendance.	textbook updates whenever required. recent order dated January 2017)	
		2c: The clinical coding standards refresher, specialty and update workshops are delivered by a Clinical Classifications Service approved clinical coding trainer using only materials endorsed by the Clinical Classifications Service or developed in accordance with national clinical coding standards.	2c	A copy of the attendee's specialty or update course certificate of successful completion / attendance. Confirmation of approved clinical coding trainer status can be obtained from the Clinical Classifications Service by emailing information.standards@hscic.gov.uk.	• Clinical Coding training assessment document for Carol Cook and Jayne Hardcastle. • Training certificates for both Coders having undertaken refresher training.	Satisfactory.
			2c	Email from the Clinical Classifications Service confirming proof of clinical coding trainer's 'approved' status.	• Screen shot of email from the clinical coding trainers.	Satisfactory.