Avon and Wiltshire NHS
Mental Health Partnership NHS Trust

Trust Board meeting		Date:	26 April 2017

Agenda item	Title	Executive Director lead and presenter	Report author
BD/17/016	**Annual IG Toolkit Submission 2016 / 2017**	**Simon Truelove**	**Kerrie Darvill**

This report is for:	
Decision	
Discussion	
To Note	X

History

The following impacts have been identified and assessed within this report	
Equality	None
Quality	None
Privacy	None

Executive summary

This report provides an update to the Board of Directors on the annual Information Governance Toolkit assessment for 2016/17 and the internal audit outcome.

This report addresses these strategic priorities:	
We will deliver the best care	x
We will support and develop our staff	x
We will continually improve what we do	x
We will use our resources wisely	x
We will be future focussed	x

1 Introduction

1.1 The Information Governance Toolkit

The Information Governance Toolkit (IGKT) is an annual self-assessment commissioned by NHS Digital for all organisations that have access to NHS patient data. Organisations must provide assurances that they are practising good information governance and use the IGTK to evidence this.

The IGTK draws together the legal rules and central guidance set out by the Department of health policy and presents them in a single standard as a set of 45 Information Governance (IG) requirements. Trusts are required to upload appropriate evidence against each of the 45 requirements within the toolkit which determines the scores for each requirement. The scores range from level zero to three. To achieve an overall organisational rating of 'satisfactory' each requirement must be scored at level 2 or above. The Toolkit must be submitted no later than the 31st March each year.

The information governance requirements are split in to the following 6 areas:

- Information Governance management
- Confidentiality and data protection
- Information security assurance
- Clinical information assurance
- Secondary use assurance
- Corporate information assurance

The full list of requirements can be viewed in Appendix 1.

In previous submissions, it appears that evidence was submitted by 'evidence owners' and that the evidence was not checked or approved by anyone centrally. As a result of this the evidence within the Toolkit was not always appropriate and didn't meet the standards specified in the toolkit guidance.

2 Information Governance Toolkit Annual Return 2016 / 2017

2.1 Summary of the work carried out

- The I.G. Toolkit review work commenced in December 2016 for the Trust, in preparation for the submission deadline of the 31st March 2017.

- Each of the 45 toolkit requirements were reviewed by the Trust I.G. lead (Kerrie Darvill), the I.G. toolkit administrator (Julie Benfell) and the Information Security and technical assurance manager (Richard Burge) and evidence was defined for each section of the Toolkit.

- IGTK spreadsheets were produced identifying the evidence required, named leads and target dates for each of the 45 requirements.

- Evidence leads were contacted on a weekly basis to discuss the evidence / requirements and submit evidence.

- A training day was held for the key information asset owners and administrators.

- A 3 week review of all of the submitted evidence was carried out by the I.G. lead to ensure that the evidence was fit for purpose. Where evidence was not fit for purpose the leads were asked to amend the evidence or if gaps still existed the I.G lead produced the required information with support from the project manager.

- Monthly progress reports (including highlighting the risk areas) were submitted and reviewed at the Information Governance Steering group.

- During the review, it was discovered that the Trust had historically classified the clinical coding standards as not applicable to the organisation (as the focus had been on clustering). On investigation, it was confirmed that these standards are relevant to mental health Trusts and as such evidence would be required to meet the standards in the toolkit. This was also verified with other mental health trusts who do meet the clinical coding standards.

- Additional resource was allocated from the IT department to ensure all the required work was carried out within the timescales e.g. Business Analysts carried out the data flow mapping exercise for each of the Trust key assets.

- Support from the IG/Information security staff was provided to the key asset owners as this was the first time that they had been required to carry out all the aspects of the information asset ownership standards appropriately.

- Prior to submitting the final Toolkit, the Trust's internal auditors (RSM Tenon) audited a sample of 6 requirements within the Toolkit. The standards that were audited were as follows:
    - 14-101 (I.G framework)
    - 14-111 (employment contracts)
    - 14-205 (subject access requests)
    - 14-300 (I.G skills and knowledge)
    - 14-401 (NHS number)
    - 14-507 (data accuracy checks)

The audit opinion for all of the six standards above was: Agree - *'From the evidence available we are able to agree the score recorded as a reasonable assessment of current performance.'*

See Appendix 2 (page 10) for the final audit report.

- The final I.G. Toolkit was submitted on Monday 27th March 2017 (this included the annual statement of assurance).

2.2 Final toolkit assessment results for 2016 / 2017

- The overall result for the 2016 / 2017 Toolkit (version 14 assessment) was 64% with a final score of 'not satisfactory'.
- The 'not satisfactory' score was a result of the Secondary use assurance section of the toolkit not achieving level 2 compliance (Relating to two clinical coding standards).
- The below table shows a breakdown of the overall score for each requirement section:

Section of the I.G. Toolkit	Level 1	Level 2	Total no. of requirements	Overall score	Final score
Information governance management	0	5	5	66%	Satisfactory
Confidentiality and data protection assurance	0	8	9	66%	Satisfactory
Information security assurance	0	15	15	66%	Satisfactory
Clinical Information Assurance	0	5	5	66%	Satisfactory
Secondary use assurance	1	6	8	54%	Not satisfactory
Corporate Information assurance	0	3	3	66%	Satisfactory
OVERALL SCORE	**1**	**42**	**45**	**64%**	Not satisfactory

2.3 Improvement plan for 2016 / 2017 non level 2 compliant section of the Toolkit

- The secondary Use assurance section within the Toolkit failed to make level 2 compliance for all the standards within it.
- An improvement plan for the clinical coding standards within the secondary use assurance section of the Toolkit was submitted to NHS Digital along with the Toolkit final submission. This will be managed via IGSG and the timescales for implementation will be agreed.
- The issues that need to be worked on to achieve level 2 in the clinical coding standards involve the following:
    - Achieving the set quality coding standards for inpatient diagnosis recording
    - Training clinicians/coders on the ICD 10 coding regulations.
- See Appendix 3 (page 19) for the Secondary use assurance improvement plan.

- There were areas of the toolkit that evidence and processes were enough to meet level 2 but that further improvement is required. These include the following:
    - Data quality
    - Corporate Information
    - Procedures
    - Information Sharing Agreements
    - Records Audits
    - IG Communications

All of the above will be included in the 17/18 IG Improvement Plan.

2.4 Improvement plan for 2017 / 2018 Toolkit

The planned work for the 2017 / 2018 will be:

- To review the trusts key assets (propose to include all the clinical systems being utilised and Ourspace)
- An improvement plan will be produced and implemented for all standards of the Toolkit with the aim of improvement in 17/18.
- The Information Governance Steering Group will oversee this process and progress will be monitored on a monthly basis.

3 Conclusion

3.1

It is clear that the previous mechanisms in place for the management and ownership of the IG toolkit in the organisation weren't adequate in order to effectively comply with the requirements of the IG toolkit. However, the actions that have taken place over recent months in order to ensure that the IG culture in the Trust is robust and the review and QA process that is required for the production of evidence for the toolkit does put the Trust in a strong position moving forward.

Information Governance needs to continue to be a focus of the organisation and the work required to meet the national standards should be carried out on an ongoing basis throughout the financial year.

4 Action

4.1

The Trust Board is asked to note and consider this report.

Appendix 1 – Mental Health Trust Full requirements list - Version 14 (2016-2017)

Req No	Description
Information Governance Management	
14-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda
14-105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans
14-110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations
14-111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation
14-112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained
Confidentiality and Data Protection Assurance	
14-200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs
14-201	The organisation ensures that arrangements are in place to support and promote information sharing for coordinated and integrated care, and staff are provided with clear guidance on sharing information for care in an effective, secure and safe manner
14-202	Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected
14-203	Patients, service users and the public understand how personal information is used and shared for both direct and non-direct care, and are fully informed of their rights in relation to such use
14-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data
14-206	Staff access to confidential personal information is monitored and audited. Where care records are held electronically, audit trail details about access to a record can be made available to the individual concerned on request
14-207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations
14-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines
14-210	All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements
Information Security Assurance	

14-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs
14-301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed
14-302	There are documented information security incident / event reporting and management procedures that are accessible to all staff
14-303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority
14-304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use
14-305	Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems
14-307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy
14-308	All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers
14-309	Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures are in place
14-310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error
14-311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code
14-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely
14-314	Policy and procedures ensure that mobile computing and teleworking are secure
14-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures
14-324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate
Clinical Information Assurance	
14-400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience
14-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements

14-402	Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care
14-404	A multi-professional audit of clinical records across all specialties has been undertaken
14-406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records
Secondary Use Assurance	
14-501	National data definitions, standards, values and data quality checks are incorporated within key systems and local documentation is updated as standards develop
14-502	External data quality reports are used for monitoring and improving data quality
14-504	Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained
14-506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place
14-507	The secondary uses data quality assurance checks have been completed
14-508	Clinical/care staff are involved in quality checking information derived from the recording of clinical/care activity
14-514	An audit of clinical coding, based on national standards, has been undertaken by a Clinical Classifications Service (CCS) approved clinical coding auditor within the last 12 months
14-516	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards
Corporate Information Assurance	
14-601	Documented and implemented procedures are in place for the effective management of corporate records
14-603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000
14-604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken

Appendix 2 – Internal Audit report carried out by RSM Risk Assurance services LLP

AVON & WILTSHIRE MENTAL HEALTH PARTNERSHIP NHS TRUST

Information Governance Toolkit (Version 14)

DRAFT

Internal Audit Report: 11.16/17

31 March 2017

CONTENTS

Debrief held	
Draft report issued	31 March 2017
Responses received	
Final report issued	

Internal Audit team	Nick Atkinson, Head of Internal Audit Karen Williams, Risk Assurance Director Vickie Gould, Manager Sheila Pancholi, ITA Lead Keith Kemmery, Principal Consultant
Client sponsor	Kerrie Darvill, Head of IM&T
Distribution	Simon Truelove, Director of Finance Sarah Knight, Interim Company Secretary Kerrie Darvill, Head of IM&T Samantha Butler, IT Project Manager

As a practising member firm of the Institute of Chartered Accountants in England and Wales (ICAEW), we are subject to its ethical and other professional requirements which are detailed at http://www.icaew.com/en/members/regulations-standards-and-guidance.

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is solely for the use of the persons to whom it is addressed and for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

1. EXECUTIVE SUMMARY

1.1 Background

An audit of the Information Governance Toolkit (IGT) Version 14 was undertaken as part of the approved internal audit periodic plan for 2016/17. During the audit has reviewed a sample of six Information Governance Toolkit standards based on the scores to be submitted by the Trust in March 2017. It should be noted that these scores can be updated (and resubmitted) prior to the final March 2017 submission.

No gaps in evidence have been identified. The Trust would have until the end of March 2017 to further demonstrate compliance with the requirement by uploading additional evidence, although we were satisfied for the sample of indicators that we reviewed that the evidence supported the self-certified scores.

The NHS Information Governance Toolkit is a self-assessment strategic framework consisting of a range of linked initiatives (standards) which all NHS Trusts are required to complete and submit to NHS Digital on an annual basis. The toolkit evaluates the adequacy of risk management and control within the Trust and assesses progress against these initiatives. Based on the results the Trust would be assigned an attainment rating, ranging from 0 to 3 (3 being the highest and fully compliant with all criteria). Where the Trust has indicated that the necessary policies, procedures and measures are in place to meet these criteria, current supporting evidence is required to be maintained.

An integral part of the IGT assessment is the annual submission of the Statement of Compliance (SoC), which provides assurance to the NHS Digital that the Trust has robust and effective infrastructure and systems in place for handling information securely and confidentially. This annual statement is necessary to obtain and maintain connection to the NHS secure infrastructure (N3) and national services. To show the required Level of assurance, a minimum attainment of Level 2 compliance against all requirements within the IGT is required.

In addition Acute, Ambulance and Mental Health Trusts are now required to submit an annual report demonstrating their performance against the Caldicott 2 Performance Recommendations. This is relevant to the following IG Toolkit requirements:

- 101
- 200, 201, 202, 203, 205, 206
- 300, 302, 307
- 400

As the Trust has not fully implemented Caldicott 2 recommendations it has produced action plans for attaining Level 3 for the relevant IG Toolkit requirements.

As part of this audit we have reviewed the evidence maintained to show compliance with a sample of six requirements which are detailed in the table below under Section 1.3 – Key Findings. The sample was selected in collaboration with the Trust to cover both strategic and operational governance controls.

The IGT requirement initiatives considered as part of this review relate to the following control area:

- Information Governance Management (14-101, 14-111)
- Confidentiality and Data Protection Assurance (14-205)
- Information Security Assurance (14-300)
- Clinical Information Assurance (14-401)
- Secondary Use Assurance (14-507)
- Corporate Information Assurance (Not in Sample)

1.2 Conclusion

Based on the evidence available at the time of the audit, we were able to agree the score of all of the six requirements assessed against the Trust's target score for March 2017. Accordingly no further recommendations have been raised as a result of this audit. Please note that IGT requirements and scoring criteria represent a high level self-assessment of performance within the organisation. Our review and

opinion is based upon the evidence provided to us to substantiate the scores submitted in relation to these high-level requirements and criteria. Our opinions are based on the reasonableness of the scores in these circumstances and do not, therefore, imply assurance that detailed controls are adequate to meet business needs. It is possible, therefore, that more detailed audits of specific areas contained within the IGT may uncover control weaknesses that subsequently appear to contradict the opinions herein.

1.3 Key findings

The following tables highlight our assessment of the Trust's self-assessment scores based on the review of available evidence.

Assessment and Recommendations

Req No.	Description	Trust Performance Score 15 March 2017	Trust Target Score for March 2017 Submission	Evidence Supports a Minimum Assessment Level	RSM Assessment of Trust's Score
14-101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	2	2	2	Agree
14-111	Organisations need to ensure that those undertaking work on behalf of the organisation do so in a lawful manner and meet all appropriate Information Governance (IG) requirements. It is vital therefore that the contracts of permanent, temporary, and locum staff contain clauses that clearly identify responsibilities for confidentiality, data protection and information security. Organisations must take reasonable steps to vet staff and provide IG training, or request appropriate training is undertaken before permitting them to access systems and information	2	2	2	Agree
14-205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	2	2	2	Agree
14-300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	2	2	2	Agree
14-401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	2	2	2	Agree
14-507	The secondary uses data quality assurance checks have been completed	2	2	2	Agree

Assessment Explanation

Agree	From the evidence available we are able to agree the score recorded as a reasonable assessment of current performance.
Understated	From the evidence provided it is our assessment the organisation is performing at a Level higher than recorded.

2 DETAILED FINDINGS - IG TOOLKIT IMPROVEMENT PLANS AND REPORTING

Result of review of the Trust plans for achievement and maintaining of Level 2 score and plans to improve scores.

Ref	Controls (actual and/or missing)	Adequate control design (yes/no)	Findings summary	Priority	Actions for management
Risk - Non-compliance with the IG Toolkit requirements					
2.1	**The robustness of the IG Toolkit improvement plans, including the monitoring and reporting of these and compliance with the 3-stage reporting timescale set by NHS Digital.** The Trust uses excel spreadsheets to record and monitor evidence requirements and track progress. The Trust are aware of, and complaint with, the 3-stage reporting timescale set by NHS Digital and takes measures to conform to such a timescale.	Yes	We found detailed spreadsheets and reporting documents from the Trust outlining the current status of each requirement and the requirement owner(s) where applicable. The Trust is aware of the 3-stage reporting timescale set by NHS Digital and we found no evidence to suggest non-conformity to such timescales. The Trust's deadlines for implementation and regular reporting schedule to the IG Steering Group shows a clear focus on IG within the organisation.	N/A	N/A

APPENDIX A: SCOPE

Scope of the Review

The internal audit assignment has been scoped to provide assurance on how Avon & Wiltshire Mental Health Partnership NHS Trust (AWP) manages the following risk:

Objective of the area under review	Risks relevant to the scope of the review
The objective of our review is to provide an opinion on the validity of a sample of IG Toolkit scores based on the evidence available at the time of audit fieldwork.	Non-compliance with the IG Toolkit requirements.

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for Consideration:

- The validity of the toolkit return based upon a review of a sample of toolkit requirements;
- Compliance with 3-stage reporting requirements; and
- The robustness of the IG Toolkit improvement plans, monitoring and reporting of these (where applicable).

Limitations to the Scope of the Audit Assignment:

- This was a sample review of the version 14 scores only. Therefore not all requirements have been examined as part of this review
- The evidence must be clearly referenced to the requirement it supports and provided at the start of the audit, otherwise we may not be able to complete any testing or provide an opinion
- As a compliance review, detailed testing was not undertaken. The operational level of the section under review was not be assessed neither was the design of the controls
- Staff surveys have not been completed to assess awareness and workplace practices

Our work does not provide any guarantee against material error, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

FOR FURTHER INFORMATION CONTACT

Victoria Gould, Manager

victoria.gould@rsmuk.com

+44(0)7740 631140

Keith Kemmery, Principal Consultant

keith.kemmery@rsmuk.com

+44(0)7837 124301

1 rsmuk.com

Appendix 3 - AWP improvement plan for the Secondary Use Assurance section of the Toolkit

Req No	Description	Current Level	Target Level	Level Description	Criteria	Criteria Description	Criteria Owner	Achieved	Criteria Actions	Evidence Required	Obtained
14-514	An audit of clinical coding, based on national standards, has been undertaken by a Clinical Classifications Service (CCS) approved clinical coding auditor within the last 12 months	1	2	Any recommendations made in previous clinical coding audits have been noted and actioned. An overall % accuracy score in a clinical coding audit of greater than or equal to level 2 scores in the guidance has been achieved.	2a	The clinical coding audit percentage accuracy scores found by the clinical coding auditors should reach level 2 scores in the table in paragraph 15 of the guidance.	Toby Rickard	No	1. Trust to agree approach to implementing 'all record' validation of relevant episodes in 2017-18 (three options: employ direct, employ via other NHS Trust or employ via third party private organisation). 2. Once agreed, engage relevant party and commence validation. 3. Once received, review recommendations from the 2016-17 audit and create an action plan to address issues identified (two items known following initial feedback are noted at points 4 and 5 below). 4. Issue clear guidance to medical workforce on diagnosis recording in RiO to ensure consistency in approach. 5. Undertake a data quality review of diagnosis records in RiO and work with the medical workforce to cleanse the data (supporting improved audit during 2017-18), focussing on the approach to allocating primary diagnosis.	A full copy of the Clinical Coding Audit Report which bears the auditor credentials has ideally been uploaded to the Information Governance Toolkit. The CCS may request reports for review from time to time to inform any changes to national standards and training.	No
14-516	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	0	2	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).	Toby Rickard	No	1. Plan for how training will be delievered, including details of attendee list for the training course and start date of the clinical coder. 2.. Agree approach to clinical coding (see 514 actions), and work with provider to evidence start of coding programme within the Trust and plan for training	Start date of coder & evidence of plan for how training will be delivered.	No
					1b	Training is delivered by approved trainer	Toby Rickard	No	1. Once traning has been delivered, obtain copy of certificate of attendance. 2. Obtain email from coding service that the trainer is approved	Evidence that the coder is trained, and that the trainer is an approved trainer.	No
				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	Toby Rickard	No	1. Develop plan for implementing refresher / awareness training	1. The plan for how the Trust ensures the right people are trained and re-trained when classifications revisions are made 2. Evidence that the training has taken place (registers) 3. Evidence that the trainer was qualified to run the sessions NB: this is applicable to both the coder and the clinicians	No
					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.	Toby Rickard	No			No
					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.	Toby Rickard	No			No