

Report to:	Board of Directors				
Date of Meeting:	27 th April 2016				
Report Title:	Annual Information Governance Service Report				
Status:	For information	Discussion	Assurance	Approval	Regulatory requirement
Mark relevant box with X	X	X	X		X
Prepared by:	Juliet Norris, Information Governance Manager				
Executive Sponsor (presenting):	Andrew Copley, Director of Finance, SIRO				
Appendices (list if applicable):	Appendix A: IG Toolkit 15_16 Score Summary Appendix B: MIAA IG Toolkit Review Airedale (1516) Appendix C: Excerpt from IG Toolkit Action Plan. Appendix D: IG Training (Face to Face) Attendee Feedback Appendix E: Support to Trust Services_Highlight Report 2015_16				

Purpose of the Report
<ul style="list-style-type: none"> • Update the Board on the Information Governance (IG) programme, confirming the results of the Toolkit assessment for 2015/16 and internal audit outcome. • Provide an overview of the arrangements in place to manage information risks and improve compliance in the year ahead. • Provide a progress summary of the activities undertaken by the IG service in-year.

Key points for information
<p>Regulatory Requirements</p> <p>All NHS Trusts are required to submit an annual assessment to the national IG Toolkit (a tool produced by the Department of Health). It enables the Trust to measure its performance through an annual self-assessment audit process and report upon levels of compliance against a set number of requirements.</p> <p>The Trust has successfully maintained a satisfactory (pass) compliance with a modest but positive increase in score from the previous year. Results are available to a number of external bodies e.g. Care Quality Commission (CQC), Monitor, Audit Commission and NHS Commissioning Board.</p> <p>Legal Requirements</p> <p>Appropriate management of activity as required under the Data Protection and Freedom of Information Acts are a requirement of all public bodies. The Trust continues to monitor, review and report on its provision of the same.</p> <p>The IG Service continues to provide support to the variety and breadth of Trust services, aiming to reduce opportunity for data breaches/losses and the ensuing fines/penalties which may follow.</p> <p>Continual Improvement - Service Activity</p> <p>The IG Service is ably supported by key roles within the Trust who provide expert guidance with regards to service policy, procedures and incident prevention and management.</p> <p>The Service is keen to build on this solid foundation by maintaining a commitment to continual</p>

improvement, and to provide quality assistance to all other Trust services.

New activity includes:

- Provision of interactive group training in IG principles and practice
- Raising the profile of the service internally; providing more support to more services and
- Externally; developing stronger links with other NHS partners, NHS England, the HSCIC, the Caldicott Council and the Chartered British Computer Society.

Recommendations

- The Board of Directors are asked to receive and note this report.

INFORMATION GOVERNANCE REPORT

1) PURPOSE

Further to reports to EAG earlier in 2016, the purpose of this report is to

- update the Board on the Information Governance (IG) programme, confirming the results of the Toolkit assessment for 2015/16 and internal audit outcome
- provide an overview of the arrangements in place to manage information risks and improve compliance in the year ahead
- provide a progress summary of the activities undertaken by the IG service in-year

2) IG TOOLKIT ASSESSMENT 2015/16

The IG Toolkit is a tool produced by the Department of Health and hosted by the Health and Social Care Information Centre (HSCIC). It draws together the relevant information management legislation and national guidance under a single framework designed to enable an organisation to implement the relevant standards. It enables the Trust to measure its performance through an annual self-assessment audit process and report upon levels of compliance against a set number of requirements. The following table lists the levels which organisations are measured against:

NR	Not relevant
0	No or insufficient evidence, not satisfactory for compliance
1	Limited evidence, not satisfactory for compliance
2	Minimum level satisfactory for compliance
3	Evidence of further processes, measures & controls, satisfactory for compliance

The Trust is required to measure itself against 45 requirements. These are broken down into the above levels and then each level contains several related sub-questions. Every answer at each level requires supporting evidence. In total this requires several hundred individual items of evidence.

Organisations can only achieve a final overall score of “Satisfactory” by scoring a minimum Level 2 for **all** requirements, regardless of the amount of progress made against individual requirements. This mechanism equates to a pass/fail outcome.

The Trust’s submission for 2015/16 took place on 31st March 2016. The Trust achieved an overall score of **Satisfactory** (Pass) with 35 criteria at the compliant level 2 and 9 criteria exceeding at level 3. Individual criteria score as detailed in Appendix A.

Prior to submitting its final assessment, the Trust’s internal auditors, MIAA audited a sample of 15 requirements within a cross-section of the Toolkit criteria. Their overall opinion was **Significant assurance**. The Board can take assurance that the controls upon which the

organisation relies to manage IG are suitably designed, consistently applied and effective. See Appendix B MIAA Audit Report.

Improvement Plan

Appendix C is an extract from the draft improvement plan showing Toolkit actions carried forward from 2015/16. New actions have also been included based on the outcome of the assessment and recommendations from the internal audit review. The plan itself is a more comprehensive “live” document forming part of the online Toolkit. It enables a requirement owner, in agreement with IG, to set and manage all actions. Actions are reviewed, progressed and monitored by the IG Group. The plan is developed and updated throughout the year.

3) COMPLIANCE WITH LEGAL AND REGULATORY FRAMEWORK

Compliance with key legislation, such as the Data Protection Act 1998 (DPA) and Freedom of Information Act 2000 (FOIA) is regulated by the Information Commissioner’s Office (ICO). Internally, the IG Group monitors compliance with the FOIA and DPA.

The Freedom of Information Act (FOIA)

Introduction

Responding to requests under the Freedom of Information Act (2000) has been the responsibility of the Head of IT & IG since mid-2011. The service is administered by one 0.8 WTE member of staff and managed by the IG Manager. The service reports to the Information Governance Group.

Activity

Under the FOI Act, anyone in the world can make a request to see information from Airedale NHS Foundation Trust. The volume of requests we receive has increased as professionals, commercial companies, press, media and the public have become more familiar with the Act. In our first full year of administration 2012/13, we received 329 requests but this has increased by 57% to a total of 571 requests received in 2015/16, an increase of 71 (an average of 5.9 extra per month) from last year. Annual growth in request volume is listed below:

Year	Volume of Requests	Percentage Growth from previous year
(June) 2011 - 2012	219	
2012 - 2013	329	+40%
2013 - 2014	502	+41%
2014 - 2015	500	Volume maintained
2015 - 2016	571	+13%

It should be noted that the volume of requests can really give no indication of the amount of time spent in answering each one. Some requests involve reporting on data that we

routinely collect and can be completed relatively quickly but others may involve large amounts of work by different departments and we frequently have to judge whether answering a request would exceed the 18 hours “appropriate cost limit”.

Public authorities should respond to a request made under the Act within 20 working days. Although our compliance continues to improve we still have some way to go to meet this target. Co-operation has improved across all departments but some requests are complex and delays can be compounded by input being required from different specialties and departments. Despite this, 83% of those responding to our feedback request say they thought the service they had received was **Good** or **Very Good**.

FOIA remains a challenge to manage and for different areas of the business to respond to.

Access to Health Records requests made under the Data Protection Act (DPA)

During 2015/16, the Trust received 1026 requests for Access to Health Records, an average of 85.5 per month. This is a reduction overall of 39 requests from 2014/15 when 1065 requests were processed. Requests come from patients themselves, their representatives, third parties and other agencies such as social services, the police and continuing care (local authorities). Request sources within the last year are detailed in the table below:

Request Type	Solicitors	Patient requests	Police	Local Authority	MIB	Health Requests	GMC	Government Agencies
TOTALS	736	176	31	15	21	31	2	14
Government Agencies	Veterans UK, Ministry of Defence, Department of Works and Pensions, Jobcentre Plus.							
Local Authorities	Metropolitan Councils, Social Services.							
Health Requests	NHS and Private Hospitals. Continuing care, Clinical Genetics Services, Cancer Research UK							
MIB	Motor Insurance Bureau							

There were 22 breaches of the 40 day response time; often due to staff shortages in the areas where records are locally held. The service ensures that customers are made aware of any potential delays. The department is not aware of any complaints being received in relation to the service.

The right of access to health records is governed by rules set out under DPA. Requests must be processed under their own individual merit and Data Controllers must consider whether each request meets the lawful requirements for provision. Many requests are straightforward but some are complex and require expert review to ensure the confidentiality rights of the data subject (and any associated third parties) are maintained. Safeguarding rules are also often applicable within this work. With regards to complex or unusual requests, the Access to Health records team bring queries to the IG Service Manager on a case by case basis throughout the year, for bespoke advice. The two services

have developed a closer relationship over the last 12 months, providing further benefit with regards to meeting the tight deadlines required under this legislation.

4) INFORMATION GOVERNANCE INCIDENTS

The Trust reported one Serious Information Governance Reportable Incident (SIRI) during 2015/16. The demographic details and some associated clinical information of 868 patients were disclosed in error and sent to 14 separate Commissioners across England. This also included a number of GP practices who were in receipt of the information from these Commissioners. The information was sent via separate Excel files from the Trust's Information team direct to a Trust partner organisation that in turn processed the information and re-sent to the expectant Commissioners. Upon discovery of the breach, the disclosed data was tracked and recovered by the Trust.

The incident was graded at level 2 in accordance with the national IG Serious Incident Requiring Investigation (SIRI) tool and reported externally to the Information Commissioner's Office (ICO) and Department of Health.

The incident was logged and managed via the Trust internal process. The SIRI was then selected for review by the Information Commissioner's Office (ICO). The Trust complied fully with the ICO process who then concluded their investigation in January 2016 with no further actions required although they did provide recommendations for the Trust to implement, listed below:

1. Ensure staff members are given reasonable deadlines and timeframes when handling or processing sensitive personal data.
2. Ensure staff members receive Information Governance Training before taking up their duties in handling personal data.
3. Ensure that relevant staff members are given sufficient training in relation to data anonymisation. Guidance on this issue is available from the ICO website: <https://ico>.

These recommendations are reviewed and monitored by the IG Group.

5) RISK MANAGEMENT AND ASSURANCE

The SIRO is responsible for overseeing the development and implementation of the information risk strategy. The SIRO is supported in this by the Information Governance team and by Information Asset Owners (IAO) within each business area. The IAO is responsible for managing information risks to the assets within their control. This involves developing system security policies (SLSP) and business continuity plans as well as documenting their personal data information flows and conducting regular information risk assessments.

The Head of IT and IG and the IT Management team support IAOs in achieving these objectives. Whilst progress has been made again during 2015/16, further work is required to embed these processes further.

The IG Toolkit is a standing agenda item for the IG Group. Requirement owners must alert the Group to any high risks, that is where the completion of certain actions are critical to achievement of Level 2, and where there are significant concerns that actions may not be completed. These are managed through a local risk register, are highlighted to the SIRO, included in any reporting, and escalated if appropriate.

IG risks are also tracked via the IT Department Risk Register which is reviewed regularly by the IM&T Management team.

6) PROGRESS IN 2015/16

IG TRAINING

In July 2015 the IG Service launched an alternative method for Trust staff. Staff may now choose to undertake the e-learning IG module provided by the Health and Social Care information Centre (HSCIC) or attend a trainer-led classroom session which includes additional focus on IG in practice, within Airedale Trust services. The trainer-led sessions are interactive in nature and have received overwhelmingly positive feedback from attendees. Over the last 8 months the IG team have delivered 53 classroom sessions to 423 employees and 993 employees have successfully completed the e-learning module.

During 2015/16 a new compliance target of 80% for all mandatory training was set by the HR department.

End of year figures from HR state that IG Training Compliance is at 69.45% at end of Q4 in 2016. The final in-year compliance for 2014/15 was 44.38%. This shows an improvement of over 25% in-year.

Feedback from attendees has been overwhelmingly positive, including (anonymous) statistics as detailed in Appendix D.

RAISING THE PROFILE

The IG Service has worked to provide an accessible forum for Information Rights and Practice advice and support to Trust services. To raise awareness of the available services the IG staff have attended a variety of clinical and corporate areas to offer Q&A sessions, to provide specialist advice regarding data sharing and to encourage confidence in handling personal information safely.

In October 2015 the IG Service represented Airedale NHS Foundation Trust at the national Caldicott conference (with Dame Fiona Caldicott in attendance), speaking about the working relationships of the IG and Caldicott functions and promoting the Airedale brand.

Additional external links such as membership of the national IG Alliance - as an Expert Reference Member – and appointment as a panel member of the (Chartered) British Computer Society’s Information Privacy Panel, continue to provide valuable exposure to further expertise and opportunity to continue to promote Airedale and its achievements. Examples include contributing to the Department of Health’s Records Code of Practice national review and bespoke supporting guidance regarding modernising the management of the health records of adopted children.

It is the sincere determination of the IG service to demystify the sometimes complex legislation regarding Information Rights and to provide practical solutions which support the delivery of care. Examples include supporting new ways of communicating with Speech & Language Therapy patients, and promoting IG principles as reliable enabling tools, rather than a barrier to progress.

SUPPORTING TRUST SERVICES

The IG Service reports Strategic Priorities, Key Risks and Mitigations, Programme and Project updates, FOIA compliance statistics and a summary of IG Expertise provided to Trust services, monthly to the Trust Digital Futures Group. Services directly supported by the IG function. Highlight report is included in Appendix E.

7) NATIONAL DEVELOPMENTS IN THE INFORMATION RIGHTS ARENA

We must continue to respond to the challenges faced by changing working practices in order to ensure that we keep pace with the ever-changing information society we work in.

Going forward, this will only become even more demanding. National developments will have a bearing on the direction of the Information Governance programme.

- **The (EU) General Data Protection regulation:** EU reforms to Data Protection regulations are expected to be published in Spring 2016. Organisations will have approx. 2 years to implement the reforms.

By way of commitment to continual improvement for the IG service, the IG Manager intends to undertake further formal study to provide ongoing expertise to the Trust in the increasingly complex area of Information Rights Law and Practice within Healthcare.

- **The 7th Caldicott Principle (Calidcott2)** continues to influence changes in data sharing practices.

“Principle 7.

The duty to share information can be as important as the duty to protect patient confidentiality”

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

- **New powers given to the ICO:**

From 1 February 2015, the ICO has been able to subject public healthcare organisations to a compulsory audit. These compulsory audits have previously only applied to central government departments.

The audits review how the NHS handles patients' personal information, and can review areas including security of data, records management, staff training and data sharing.

The ICO can assess how information governance is applied and embedded by England's NHS foundation trusts, GP surgeries, NHS Trusts and Community Healthcare Councils, and their equivalent bodies in Scotland, Wales and Northern Ireland under section 41A of the Data Protection Act.

To date, the ICO has issued fines totalling £6.4m to NHS and Health organisations.

- **Freedom of Information Act (national review)**

The Independent Commission on the Freedom of Information Act reported its findings on 1st March 2016 having considered over 30,000 responses to their call for evidence from both data providers and requesters.

There are no significant changes to Act in their recommendations but there is a proposal that organisations with over 200 employees should begin to publish their responses to FOI requests online. Whilst this seems sensible, our evidence shows that less than half of requesters would check an organisation's website before sending a request for information and around 60% of those responding to our request for feedback, have sent the same request to all Acute Trusts in England.

8) SUMMARY

The Trust has a robust process for managing IG and the associated responsibilities that come with our commitment to adopt best practice processes and procedures in order to protect patient and service users' information. It has a dynamic action plan to refresh and improve its compliance with the Toolkit standards.

Evidence for many of the requirements is refreshed as part of established daily business or monitoring activities. However, some objectives are more challenging and for this reason are being targeted already. Key areas identified below:

Area	Rationale
Promote and monitor the uptake of IG training	An organisation's approach to IG Training provision is a frequent key factor when the ICO consider potential enforcement action during their investigations of IG SIRIs, <i>regardless</i> of the nature of the actual reported incident.
Continue embedding Information Governance best practice within the culture of the organisation, through additional awareness and training	Prevention of IG breaches and SIRIs. Raise confidence within service areas and empower staff to recognise and respond to IG matters as they arise.
Review and update the annual information workflow exercise to capture new flows, and ensure that data sharing agreements and/or appropriate IG controls are in place, specifically ensuring the organisation logs and tracks the legal basis underpinning its data flows.	Compliance with IG Toolkit criteria: 110 <i>Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations</i> 308 <i>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</i>
Review the Trust contracts register to ensure key contracts are aware of updated IG clauses.	Compliance with IG Toolkit criteria: 207 <i>Where required, protocols governing the routine sharing of personal information have been agreed with other organisations</i> 308 – <i>as above</i>
Support the Trust's strategy and management of data quality	Compliance with IG Toolkit criteria: 402 <i>Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care</i> 506 <i>A documented procedure and a regular audit cycle for accuracy checks on service user data is in place</i>
Work with the Caldicott and Risk department to target IG incident 'near misses' with a view to reducing the potential for IG SIRIs	To protect patient information, other associated Trust assets and to mitigate against potential fines / sanctions.
Work with IAOs to embed effective information risk	To protect patient information, other associated Trust assets and to mitigate against potential fines / sanctions.

management activities	
Engage with Patients/members of the public, raising the profile of Information Rights, Consent, Dissent and associated opinion from users of the Trust's services.	To inform and improve the national mandate for all NHS organisations to provide Fair Processing Notices for all patients and members of the public. Compliance with IG Toolkit criteria: 203 <i>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</i>
Strengthen inclusion of IG principles and guidance within the Trust's overarching and local Business Continuity Planning processes and key supporting documentation.	Compliance with IG Toolkit criteria: 309 <i>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</i>

We will continue to work with other NHS organisations in our region sharing good practice, and to aim for an integrated approach.

The IG Group asks the Board to receive and note this report. It is asked to support plans to ensure that the Trust achieves an overall satisfactory position by achieving a minimum Level 2 for all IG Toolkit requirements for 2016/17 and crucially, that it continues to improve and embed best IG practice into routine working practice across the Trust.

12 April 2016

Juliet Norris, IG Manager
On behalf of Tim Rycroft, Head of IG and IT

Totals			
	Criteria at Level 2	Criteria at Level 3	Overall Percentage score
2014/15	37	7	71%
2015/16	35	9	73%

Criteria Ref	Criteria Detail	Notes	Score
Information Governance Management			
101	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda	Substantiated by Audit. IG Service considers that local evidence demonstrates compliance at level 3.	Level 3
105	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans	Maintained from previous year	Level 3
110	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations	Substantiated by Audit. IG Service considers that local evidence demonstrates compliance at level 3.	Level 3
111	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation	Maintained from previous year	Level 2
112	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained	Increase from Level 2 in 2015/16	Level 3

Confidentiality and Data Protection Assurance			
200	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs	Maintained from previous year	Level 3
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	Maintained from previous year	Level 2
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	Not substantiated by Audit. IG Service considers that local evidence demonstrates compliance at level 2, whilst acknowledging there is room for further development in 2016/17.	Level 2
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	Substantiated by Audit.	Level 2
205	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data	Level 3 requires provision of online access for patients to their health records, without charge. IG Service to consider if/when this may be achievable.	Level 2
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	Substantiated by Audit. IG Service considers that local evidence demonstrates compliance at level 3. Audit processes for non-key	Level 3

Appendix A_2015/16 IG Toolkit Score Summary

		systems to be reviewed in 2016/17.	
207	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations	Substantiated by Audit.	Level 2
209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	This criteria is Not Applicable to ANHSFT. Therefore 'N/R' is selected during submission.	N/R
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	Maintained from previous year	Level 2

Information Security Assurance			
Criteria Ref	Criteria Detail	Notes	Score
300	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs	Maintained from previous year	Level 2
301	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed	Maintained from previous year	Level 2
302	There are documented information security incident / event reporting and management procedures that are accessible to all staff	Substantiated by Audit.	Level 2
303	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority	Maintained from previous year	Level 2
304	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use	Substantiated by Audit.	Level 2
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	Maintained from previous year	Level 2
307	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	Maintained from previous year	Level 2
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	Substantiated by Audit at level 1. IG Service consider that local evidence demonstrates compliance at level 2.	Level 2
309	Business continuity plans are up to date and tested for all critical information	Substantiated by Audit.	Level 2

Appendix A_2015/16 IG Toolkit Score Summary

	assets (data processing facilities, communications services and data) and service - specific measures are in place	Recommendations to strengthen IG references within Trust BCP processes agreed to take forward to 2016/17.	
310	Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error	Maintained from previous year	Level 2
311	Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code	Substantiated by Audit.	Level 2
313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Maintained from previous year	Level 2
314	Policy and procedures ensure that mobile computing and teleworking are secure	Maintained from previous year	Level 2
323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Maintained from previous year	Level 2
324	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Maintained from previous year	Level 2

Clinical Information Assurance			
Criteria Ref	Criteria Detail	Notes	Score
400	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience	Maintained from previous year	Level 2
401	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements	Maintained from previous year	Level 2
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	Substantiated by Audit at level 2. Health Records service considers that local evidence demonstrates compliance at level 3.	Level 2
404	A multi-professional audit of clinical records across all specialties has been undertaken	Maintained from previous year	Level 2
406	Procedures are in place for monitoring the availability of paper health/care records and tracing missing records	Maintained from previous year	Level 3

Secondary Use Assurance			
Criteria Ref	Criteria Detail	Notes	Score
501	National data definitions, standards, values and validation programmes are incorporated within key systems and local documentation is updated as standards develop	Maintained from previous year	Level 2
502	External data quality reports are used for monitoring and improving data quality	Maintained from previous year	Level 2
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	Maintained from previous year	Level 2
505	An audit of clinical coding, based on national standards, has been undertaken by a Clinical Classifications Service (CCS) approved clinical coding auditor within the last 12 months	Substantiated by Audit.	Level 2
506	A documented procedure and a regular audit cycle for accuracy checks on service user data is in place	Substantiated by Audit.	Level 2
507	The Completeness and Validity check for data has been completed and passed	Maintained from previous year	Level 2
508	Clinical/care staff are involved in validating information derived from the recording of clinical/care activity	Maintained from previous year	Level 2
510	Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards	Maintained from previous year	Level 2

Corporate Information Assurance			
Criteria Ref	Criteria Detail	Notes	Score
601	Documented and implemented procedures are in place for the effective management of corporate records	Maintained from previous year	Level 2
603	Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000	Substantiated by Audit.	Level 3
604	As part of the information lifecycle management strategy, an audit of corporate records has been undertaken	Maintained from previous year	Level 2

IG Toolkit Review Assignment Report 2015/16

Airedale NHS Foundation Trust



CELEBRATING
25 YEARS
OF MIAA

Contents

1. Introduction, Background and Objectives
2. Executive Summary
3. Findings, Recommendations and Action Plan

Appendix A: Validity of Returns

Appendix B: Terms of Reference

Appendix C: Assurance Definitions and Risk Classifications



1. Introduction, Background and Objective

This review was planned and undertaken to provide an opinion upon the policies and processes established by the Trust to develop and embed an Information Governance (IG) culture within the organisation, to collate and submit its IG return and to provide an independent assessment of the validity and accuracy of the scores submitted. This objective and a more detailed scope are provided within Appendix B of this report.

2. Executive Summary

The following provides a summary of the key themes.

Internal Governance Process

The Trust has a clear organisational IG structure and there are processes for identifying, improving and embedding IG in the organisation.

Key staff roles support the IG structure. The Director of Finance is the Trust Senior Information Risk Owner (SIRO). The IT Clinical Director is the Trust Caldicott Guardian. The SIRO supports the Chief Executive and the Board in ensuring compliance with appropriate standards and managing information risks. Freedom of Information compliance is managed by the Head of IT and IG with responsibility for ensuring that procedures and processes are in place.

There is an established Information Governance Group (IGG) which oversees IG compliance, manages issues and incidents and reports on action plans and projects. The Head of IT and IG chairs the IGG. Membership includes the SIRO, Caldicott Guardian and other senior representatives across the Trust.

The IGG is accountable to the Executive Assurance Group.

The IGG regularly reports and informs on progress and compliance with the IG Toolkit and the SIRO signs off the 31st March annual submission.

Validity of Returns

The audit review for the 2015/2016 IG Toolkit submission was carried out in two phases. Phase one took place in November 2015. The auditor was provided with access to the evidence which supported the 15 sample requirements agreed by the Trust, and as set out in Appendix B of the MIAA 2015/2016 Terms of Reference.

The initial audit findings were provided in the form of a spreadsheet to the Information Governance Manager and IT Customer Support.

The second phase of the audit was carried out in February and March 2016. The purpose was to review any additional evidence and clarification that had been provided, following the initial assessment.

This report contains the audited assessment of the evidence provided to date.

In 11 of the requirements reviewed we were able to confirm that the score to be submitted was at, or above, the minimum mandated compliance level and reasonable in light of the currently available

evidence. In our opinion, a total of 4 were unsubstantiated at the required level 2 and 3 out of 4 claimed at level 3 were not adequately substantiated at this level.

The following table shows a summary of our opinion of the Trust's self-assessment of the score achieved against each requirement.

Self-Assessment Score	Our Opinion		
	Agreed	Unsubstantiated	Overstated
Not Relevant	-	-	-
0	-	-	-
1	-	-	-
2	9	2	-
3	1	3	-

The opinions given on these requirements are based on the definitions set out in the national guidance's approach to the IG Toolkit Review, these definitions and their meaning can be found in Appendix C.

Wider risk exposure/mitigation

For identified gaps an IGT action plan is recommended and each action with a named lead person and completion date. The action plan should be monitored by the IG team, to ensure that all deliverables are completed by the required dates.

In a number of requirements, although we have agreed the submission score, we have highlighted some areas of potential improvement which the Trust may wish to consider as part of its on-going IG work programme.

In the wider sense there is still some opportunity for improvement in interpreting the requirements correctly and focusing in on the most effective subset of evidence to make the tool set process as effective as possible.

Conclusion

A number of gaps and opportunities for improvement were identified and management should assure themselves that the actions being undertaken to mitigate these aspects are completed in a timely manner and with the desired effect. Particular areas of concern revolved around the identification and control of data flows which undermined 3 requirements, but this is acknowledged to have been due to staffing issues in the responsible area. Other gaps were spread across different control disciplines.

There are some weaknesses in the design and/or operation of controls which could impair the achievement of the objectives of the system, function or process. However, either their impact would be minimal or they would be unlikely to occur. In light of the findings the level of assurance provided is:

Significant Assurance

It should be noted however, our review and opinion is based upon the evidence provided to us to substantiate the scores submitted in relation to the high level requirements and criteria. Our opinions are also based upon the reasonableness of the scores in these circumstances and do not, therefore, infer assurance that detailed controls are adequate to meet business needs. It is possible, therefore, that more detailed audits of specific areas contained within the IG Toolkit may uncover control weaknesses which subsequently appear to contradict the opinions herein.

Appendix A: Validity of Returns

IG Req. No.	13-101
	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda
Trust Score	3
Our Opinion	Unsubstantiated
Rationale	Level 1 Agreed It is recommended that responsibility for leading the IG work area be assigned to the SIRO, Caldicott Guardian or an Executive Director. Level 2 Agreed Assuming evidence of key forum activity in current year is made available. Level 3 – Unsubstantiated Evidence of senior management involvement in wider IG arrangements required.
IG Req. No.	13-110
	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations
Trust Score	2
Our Opinion	Agreed*
	* Internal approval of the use of NHS Terms and Conditions IG clauses within the Trust is expected. In addition, it is acknowledged that contracts on earlier NHS Terms and Conditions, or non-NHS, have been identified and the review is ongoing with a risk assessment due end of March 2016.
IG Req. No.	13-202
	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
Trust Score	3



122AFT_1516_901

Our Opinion Unsubstantiated

Rationale

Level 1 – Unsubstantiated

A simplistic project plan provided but this is not the sort of plan expected which should explain the process and approach in line with the guidance.

Level 2 – Unsubstantiated

Legal admissibility was not covered in initially evidenced process and whilst this gap was acknowledged and action taken to correct it, it should have been well embedded previously. It is expected to be more or less complete by submission.

Level 3 - Unsubstantiated

Satisfaction surveys that specifically evidence that service users understand their consent choices are required.

IG Req. No.

13-203

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

Trust Score

2

Our Opinion

Agreed*

* Assuming relevant communication materials will be presented to, and agreed by, the Patient Engagement Forum by end of March 2016. The wider action plan re improved activity and engagement in this area should be progressed as anticipated.

IG Req. No.

13-206

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

Trust Score

2

Our Opinion

Agreed*



Clinical Systems Manager responsibilities in this regard could be clearer and better aligned to IG requirement expectations. Evidence for level 3 requires strengthening by including audit trails and system logs for more key systems.

IG Req. No.	13-207
	Where required, protocols governing the routine sharing of personal information have been agreed with other organisations
Trust Score	2
Our Opinion	Unsubstantiated
Rationale	<p>Level 1 – Unsubstantiated</p> <p>Responsibility of developing suitable sharing protocols should be assigned to an individual or group.</p> <p>Data Flow spreadsheet is incomplete particularly the IG/ISO compliance and purpose of sharing columns, which should have been well established, however, the exercise to correct this is ongoing.</p> <p>Level 2 – Agreed</p> <p>As stated above, the Data Flow exercise is ongoing. High level protocols for information sharing partners on the spreadsheet that are unable to demonstrate compliance should be signed off by senior management.</p>

IG Req. No.	13-302
	There are documented information security incident / event reporting and management procedures that are accessible to all staff
Trust Score	2
Our Opinion	Agreed*
Rationale	<p>* Whilst we accept that an IG SIRI process is operating, and demonstrably so, in terms of identifying and reporting incidents in line with HSCIC standards localised provision of linked procedures and guidance requires attention. An element of this requirement relating to contracts is impacted by 110 which is an ongoing process.</p>



IG Req. No.	13-304
	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use
Trust Score	2
Our Opinion	Agreed
	*Assuming revised RA plan/procedures will be approved by IG Group March 2016.

IG Req. No.	13-308
	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
Trust Score	2
Our Opinion	Unsubstantiated
	Level 1 – Agreed.
	However, whilst the process currently underway demonstrates appropriate actions and activities are in hand an appropriately approved plan/policy/procedure to underpin the process of ensuring the transfers of sensitive data is risk assessed and adequately mitigated is required.
	Level 2 – Unsubstantiated
	The process is currently ongoing to recreate and enhance the data flow controls in line with this requirement and other dependent items. The risk assessment element and mitigation is not adequately clear.

IG Req. No.	13-309
	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
Trust Score	2

Our Opinion Agreed – but existing strategy, whilst good, requires enhancing to fully integrate IG elements. SIRO is required to approve BCPs in the IG context and tracking of IG approved BCPs in place is expected. The existing strategy has been approved by senior management but as it is not fully IG compliant it undermines the assurance in this respect. Finally, feedback from the IG aligned BCP process should feed back to the SIRO and/or risk registers, where appropriate.

IG Req. No. **13-311**
Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code

Trust Score 2

Our Opinion Agreed.

IG Req. No. **13-402**
Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care

Trust Score 3

Our Opinion Unsubstantiated

Rationale Level 1 – Agreed, but evidence could be better aligned to requirement in terms of procedures not strategy. Furthermore, full minutes expected not one paragraph in isolation.

Level 2 – Agreed, but evidence of procedures/strategies targeting staff involved in data collection could be better.

Level 3 – Unsubstantiated – system data quality checks evidenced but compliance with procedures and understanding checks are required.

Evidence that data collection and validation activities and compliance checks are carried out is required.

IG Req. No. **13-505**
An audit of clinical coding, based on national standards, has been



undertaken by a Clinical Classifications Service (CCS) approved clinical coding auditor within the last 12 months

Trust Score 2

Our Opinion Agreed

IG Req. No.

13-506

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

Trust Score 2

Our Opinion Agreed - but responsibility, evidence quality and alignment to IG needs to be much stronger.

Rationale

IG Req. No.

13-603

Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000

Trust Score 3

Our Opinion Agreed

Level 1 – Agreed

Level 2 - Agreed

Staff could benefit from some proactive reminders via newsletters, briefings and global comms.

Level 3 - Agreed

Appendix B: Terms of Reference

The objective of our review was to provide an opinion on the adequacy of policies, systems and operational activities to complete, approve and submit the IG Toolkit scores. We also provided an opinion on the validity of the scores based on the evidence available.

Scope of Work

Our work was undertaken in phases. It aimed to assess and provide assurance based upon the organisational IG infrastructure, the validity of its intended March 2016 submission to help consider not only if the scores claimed are reasonable based on the evidence submitted, but also provide assurance based on the extent to which information risk has been managed in this context. The figure below illustrates how these elements interact to provide the organisations assurance.



Specifically the work focused upon:-

Internal Governance Process	<p>We reviewed the processes for the collation of information from across the organisation for the assessment of the IG toolkit scores including:</p> <ul style="list-style-type: none"> ▪ how the organisation is structured to assess compliance against requirements; ▪ how the returns are made to the IG Manager; ▪ how the returns are validated and moderated; ▪ how the returns are evidenced; and ▪ how the returns are signed off for submission
Validity of Returns	<p>We considered the validity of the scores to be submitted at the end of March 2016 for the selected requirements based on the evidence to support them at the time of review.</p>

Wider Risk Exposure / Mitigation	We identified any risk exposure highlighted by current practice or, where appropriate, where current activities, while not meeting the toolkit prescribed approach are such that they do meet the overarching objective of a requirement and are effectively mitigating the operational risk.
----------------------------------	---

This was in part driven by whether the organisation is meeting the minimum required compliance level of two in each scored criterion.

Limitations inherent to the internal auditor's work

We have undertaken the review of the process, subject to the following limitations.

Internal control

Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgement in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future periods

The assessment of controls relating to the process is that at March 2016. Historic evaluation of effectiveness is not always relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in the operating environment, law, regulation or other; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We shall endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected. The organisation's Local Counter Fraud Officer should provide support for these processes.

Appendix C: Assurance Definitions and Risk Classifications

Level of Assurance	Description
High	Our work found some low impact control weaknesses which, if addressed would improve overall control. However, these weaknesses do not affect key controls and are unlikely to impair the achievement of the objectives of the system. Therefore we can conclude that the key controls have been adequately designed and are operating effectively to deliver the objectives of the system, function or process.
Significant	There are some weaknesses in the design and/or operation of controls which could impair the achievement of the objectives of the system, function or process. However, either their impact would be minimal or they would be unlikely to occur.
Limited	There are weaknesses in the design and / or operation of controls which could have a significant impact on the achievement of the key system, function or process objectives but should not have a significant impact on the achievement of organisational objectives.
No	There are weaknesses in the design and/or operation of controls which [in aggregate] have a significant impact on the achievement of key system, function or process objectives and may put at risk the achievement of organisational objectives.

Risk Rating	Assessment Rationale
Critical	Control weakness that could have a significant impact upon, not only the system, function or process objectives but also the achievement of the organisation's objectives in relation to: <ul style="list-style-type: none"> • the efficient and effective use of resources • the safeguarding of assets • the preparation of reliable financial and operational information • compliance with laws and regulations
High	Control weakness that has or is likely to have a significant impact upon the achievement of key system, function or process objectives. This weakness, whilst high impact for the system, function or process does not have a significant impact on the achievement of the overall organisation objectives.
Medium	Control weakness that: <ul style="list-style-type: none"> • has a low impact on the achievement of the key system, function or process objectives; • has exposed the system, function or process to a key risk, however the likelihood of this risk occurring is low
Low	Control weakness that does not impact upon the achievement of key system, function or process objectives; however implementation of the recommendation would improve overall control.

Report Distribution

Name	Title	Report Distribution
Andrew Copley	Director of Finance	PDF
Tim Rycroft	Head of Information Technology & Information Governance	PDF
Juliet Norris	Information Governance Manager	PDF

Discussion meeting held with

Name	Title	Date
Tim Rycroft	Head of Information Technology & Information Governance	March 2016
Juliet Norris	Information Governance Manager	March 2016



Review prepared on behalf of MIAA by

Name: Sharon Kupe

Title: IM&T Auditor

Telephone: 0151 285 4697

Email: Sharon.Kupe@miaa.nhs.uk

Name: David Orme

Title: Senior IM&T Audit Manager

Telephone: 0151 285 4530

Email: David.Orme@miaa.nhs.uk



Appendix C: Extract from IG Over-Arching Work Plan 2016/17

Important Note: this plan is pending publication of the revised 2016/17 Toolkit (v14) in Summer 2016

IGT req.	Action	Action owner	Deadline	Progress	Status
Over-Arching Objectives					
Supports whole Toolkit	Review IG Guidance for Staff and Public: includes methods of publication. Include emphasis on Trust Code of Confidentiality.	T Rycroft / J Norris	31/01/2017	Pending	open
Supports whole Toolkit	Review IG Training Materials / Methods of Delivery	T Rycroft / J Norris / with Workforce Development	31/01/2017	Pending	open
Supports whole Toolkit	Review of Trust Information Asset Register and supporting SLSP process.	T Rycroft / J Norris / IT Systems Manager	31/01/2017	Pending	open
Supports whole Toolkit	Monitor provision of fair processing posters (privacy notices) Improve communication with users of Trust services.	T Rycroft / J Norris	31/01/2017	On-going throughout the year	open
Supports whole Toolkit	Review IG Sharepoint / Intranet Presence	T Rycroft / J Norris	31/01/2017	On-going throughout the year	open
Supports whole Toolkit	Work with the Caldicott and Risk department to target IG incident 'near misses' with a view to reducing the potential for IG SIRIs	T Rycroft / J Norris	31/01/2017	On-going throughout the year	open
Criteria Specific Objectives					
110	Review the Trust contracts register to ensure key contracts are aware of updated IG clauses	Tim Rycroft Graham Beck	31/01/2017	instructions issued in part for key system	open
112 (2a)	Audit Recommendation is for the Trust to achieve 95% staff compliance with IG Mandatory training, as per the national mandate.	T Rycroft / J Norris	31/01/2017	Pending	open
207 (2b)	Review Information Sharing Protocols	IG Group	31/01/2017	On-going throughout the year	open
210 (2b)	Strengthen PID/PIA documentation for new projects	T Rycroft / J Norris	31/01/2017	Pending	open

309	Strengthen inclusion of IG Principles within Trust Business Continuity Planning. Provide support to recognise threats to Trust Information Assets and ensure escalation routes are appropriate and include SIRO.	T Rycroft / J Norris / Carol Woolgar	31/01/2017	Pending	open
202 and 308	Conduct the annual Data Flows review exercise, with inclusion of additional elements as recommended in Toolkit guidance. Ensure legal basis of transfer is checked and included in the annual outcome.	T Rycroft / J Norris / Head of Information Services	31/01/2017	On-going throughout the year	open
502 and 504	Strengthen Data Quality checks on Patient Data (Health Records) closer to point of input. Review systems to maximise opportunity for cross-checking and data reconciliation.	T Rycroft / J Norris / Head of Information Services / Head of Health Records	31/01/2017	On-going throughout the year	open

Month	How well was the purpose of today's training explained to you?					How effective was the training in describing the importance of IG to the work that you do at the Trust?					How would you rate your confidence now to report and IG concern?					How would you now rate your knowledge of IG relevant to your work at the Trust?					(Example) Attendee Comments			
	Very Poor	Poor	Satisfactory	Good	Very Good	Very Poor	Poor	Satisfactory	Good	Very Good	Very Poor	Poor	Satisfactory	Good	Very Good	Very Poor	Poor	Satisfactory	Good	Very Good				
April 2016				1	14				2	13				2	13				2	13				
March 2016			2	13	35			1	15	34			1	22	27			2	23	24			<i>Preferred this session to doing on line training</i>	
Feb 2016			1	11	36				12	36			1	15	33			1	14	31			<i>Very relaxed atmosphere - easy to participate in Felt less like a tick box exercise more informative</i>	
Jan 2016				7	31			1	5	32				11	19				13	25			<i>I preferred this way of training to just sitting behind a screen It was nice not to have the screen just read to you</i>	
Dec 2015				4	6				4	5				5	4				7	2			<i>Much prefer being taught in person - can share ideas - more friendly - and for me the information sinks in as it is my preferred learning style.</i>	
Oct 2015			2	24	91			1	23	91			3	35	76			4	35	76				
Sept 2015				1	7				1	7					8			1		7				
August 2015					9					9					9					8				
July 2015					3					3				1	2				1	2				
Totals			5	61	232			3	62	230			5	91	191			8	95	188				

Appendix E_IG Support to Trust Services – 2015/16 – Highlight Report

	Trust Service(s)	Topic(s)
Clinical Services	Womens & Childrens Pathology Medical Secretaries Safeguarding Speech & Language Therapies Paediatrics Community Services Bed Managers Maternity Services Mobility Services A&E Community Rehab AGH Ward staff	Maternity Professionals sharing via Social Media. Guidance re suspected IG Breach and subsequent disciplinary investigation. Data Sharing to National Renal Registry. Advice re provision of clinical data to patient (ANHSFT and non-ANHSFT data) Good IG Practice in patient access workspaces Advice re data sharing with Social Services Advice re data sharing (patient) data with DWP Advice re modernisation of Antenatal Notification Process Advice re communicating with SALTs patients via email/text Advice re potential video/safe storage of autism assessments Good IG Practice in patient access workspaces Advice re appropriate use of Social Media sites IG Support re data sharing transactions, take up of S1, digital record keeping standards Direction re correction of incorrect data within scanned A&E records. Guidance re use of faxes Reminders re appropriate smartcard use / associated risks
Corporate	HR Estates PALS Complaints Patient Safety Manager (Legal Services) PA to Medical Director Health Records Equality & Diversity Executive Office Supplies (re Pathology) Assistant Director of Patient Safety	Advice & Direction re Police / NMC requests for staff data. Advice on redacting confidential data for provision to ex-employee Support managing Subject Access Requests for Staff Personal Data Advice re provision of Witness Statements to ex-employee Secure disposal of Confidential Waste Set up and management of a Volunteers database Introduction to digital redaction of confidential data - method and demonstration Assistance with Audits of SI activity to support HR investigation. IG advice re use of Third Party supplier for Real Time Survey data collections. Assistance with SOP for Patient Stories: consent and storage Advice re Security and Confidentiality Safe Haven guidance Review of Contract details for proposed new shared care with BTHFT Advice re use of additional social media platforms Support to Urgent Care Vanguard re Data Sharing Support with SOPs for Clinical Photography Policy Advice re IG aspects of potentially recording Complaints process meetings

Other	Research & Development	IG Review of applications to use ANHSFT patient data in research projects (multiple) Advice re internal database for patients who may participate in future research projects.
External	Cheshire & Wirral Partnership NHS Foundation Trust BTHFT BDCT Involve/Immedicare HSCIC – IG Alliance Academic Health Science Network British Computer Society (BCS)	Advice re accessing additional IG Expertise / Training via national training tool (ANHSFT IG service recommended externally by MIAA) Data Sharing re Diabetic Eye Screening processes, with BTHFT. IG/Info Security Support re sharing IT Training Suite resources. Participation in early stage development of Cyber Security training materials, for potential national deployment. Advice re data sharing with clinical systems Advice re Consent model for Text Reminders service Assistance with E-Learning (IG Refresher) access Assistance with PIA Templates/ Data Sharing Agreements Scoring Immedicare IG breaches Developing national guidance regarding management of adopted children’s health records. Academic Health Science Network Membership of the BCS Information Privacy Panel