auditone

Humber NHS Foundation Trust

Internal Audit Report Ref: 180407
Date: 27th March 2018

Information Governance Toolkit Review (v14.1)

Contents

Section

Draft report issued	19.03.18	Audit Team	Stephen Watson, Head of Technology Risk Assurance Karen Wass, Technology Risk Assurance Manager Nikki Cooper, Principal Auditor
Responses received	26.03.18	Client Sponsor	Peter Beckwith, Director of Finance, Infrastructure and Informatics
Final report issued	27.03.18	Report distribution	Peter Beckwith, Director of Finance, Infrastructure and Informatics Hilary Gledhill, Director of Nursing, Quality & Patient Experience Lisa Davies, Head of Information Governance & Legal Services Tracey O'Mullane, Information Governance Officer Jenny Jones, Trust Secretary Michele Moran, Chief Executive (Final report only)

apply any relevant exemptions which may exist under the Act to such report where it concurs that they are appropriate. If, following consultation with AuditOne, The Trust discloses this report or any part thereof, it shall ensure that any disclaimer which Audit One has included or may subsequently wish to include in the information is reproduced in full in any copies disclosed.

AuditOne is hosted by Northumberland Tyne and Wear NHS Foundation Trust.

Our work was completed in accordance with Public Sector Internal Audit Standards.

Executive Summary

1.1 Introduction

This review was carried out in February and March 2018 as part of the planned internal audit work for 2017/18. Based on the work carried out an assessment of the adequacy of the arrangements to mitigate the key control risk areas is provided in the Executive Summary.

The Information Governance Toolkit is a Department of Health (DH) Policy delivery vehicle that NHS Digital is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DH policy and presents them in in a single standard as a set of information governance requirements. The organisations in scope of this are required to carry out self-assessments of their compliance against the IG requirements. There are 45 requirements in the toolkit completed by the Trust, each can be scored at a level 0, 1, 2, or 3, the higher the score the more mature and developed the controls in place. To ensure a "successful" rating of the toolkit submission, the organisation is required to demonstrate a minimum attainment of a level 2 score for all requirements.

This report summarises findings and impact together with details of management responses and target dates for action. We will follow up responses in line with the agreed internal audit protocol and present results to the Audit Committee.

1.2 Conclusion

At the date of our review March 2018, we identified nine requirements which could be substantiated at the level claimed. We did however note one requirement which was unsubstantiated. Differences identified by AuditOne in the level claimed are detailed in section 1.4 of this report. AuditOne acknowledges that the differences identified in the level attained may be due to timing issues and that Humber NHS Foundation Trust has until 31st March to upload all relevant to attain the level stated as per the toolkit.

1.3 Scope of the audit

The objective of the audit is to provide assurance on the integrity of the self-assessment against the toolkit criteria, the overall effectiveness of information governance processes, and wider risk exposures.

Our testing and our opinions are limited to the following sample of 10 of 35 requirements which was agreed with management:

- 14.1.101 - There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda.
- 14.1.112 - Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained.
- 14.1 200 - The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs.
- 14.1.210 - 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.
- 14.1.307 - An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy.
- 14.1.309 - 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.
- 14.1.314 - Policy and procedures ensure that mobile computing and teleworking are secure.
- 14.1.404 - A multi-professional audit of clinical records across all specialities has been undertaken.
- 14.1.506 - A documented procedure and a regular audit cycle for accuracy checks on service user data is in place.
- 14.1.604 - As part of the information lifecycle management strategy, an audit of corporate records has been undertaken.

1.4 Key Findings and Action Points

The key control findings and operational observations that need to be addressed in order to strengthen the control environment are set out in Appendix A (Findings and Recommendations). Recommendations for improvements should be assessed for their full impact before they are implemented.

The following table provides a comparative summary for the sample of the organisation's toolkit requirements reviewed during the IGT audit process. It shows the scores self-assessed by the Trust at the date we completed our review and the scores that we validated during the audit process.

Requirement Number	March 2018	
	Level Self-Assessed by Trust	Level Assessed by Auditor
101	3	3
112	3	2
200	3	3
210	3	3
307	2	2
309	3	3
314	2	2
404	2	2
506	2	2
604	2	2

We noted the following points for observation during the audit:

- The Information Governance Training Review 2017 and the IAO's Datix review will be taken to the next Information Governance Group (IG Group) in March 2018 for review and approval.
- The IG Monitoring Report 2017-18 and Emergency Preparedness Resilience & Response Annual Report 2017-18 will be completed after year end (31st March 18). We have been advised that these reports will be uploaded to the toolkit as soon as they become available.
- System Level Security Policies for Datix, Lorenzo and SystmOne which are currently in the process of being updated will be completed and signed off at future IG Group meetings.
- Confirmation is awaited that all Information Asset Owners have completed the IAO workbook and assessment by March 2018.

- We were informed that the following documents are currently under review:
  - Standard Operating Procedures For Applying For Permanent Removal Of Information From A Patients Record In SystmOne,
  - The Records Management and Information Lifecycle Policy and
  - The Health and Social Care Records Policy.

Appendix A (Key Findings and Action Plan) provides further details on the findings of the assessment of each of the requirements tested and provides recommendations to assist the Trust meet the required levels prior to the March 31st submission date.

1.5 Limitations to the scope of the audit:

Information Governance requirements and scoring criteria represent a high-level self-assessment of performance within the Trust. Audit review and opinion is based upon the evidence available to substantiate the score submitted in relation to these high-level requirements and criteria, at the time of the audit. Audit opinions are 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 provided by this report.

Although the work outlined within the Toolkit is linked to the Data Protection Act, the report does not provide any assurances in relation to compliance with the legislation. The submission of a level 2 assessment also does not provide the Trust with an assurance that a data breach will not occur. The information provided in our report should not therefore be considered to detail all errors or risks that may currently or in the future exist within the Information Governance control framework, aspects of which should be considered subject to varying degrees of change over time and our comments and opinion is be based solely on the information provided at a given point in time.

1.6 Corporate significance

Failure to achieve the minimum required standard of level 2 for each requirement may result in the ineffective management and security of data. This may have a negative impact on patients and staff and cause reputational damage as well as posing a financial risk to the Trust.

The Information Commissioner's Office has the power to issue monetary penalty notices of up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010, and serious breaches of the Privacy and Electronic Communications Regulations.

1.7 Acknowledgement

We would like to thank management and staff for their help and cooperation in the course of this audit.

2 Action Plan

Ref	Recommendation	Priority	Accepted (Y/N)	Management Action	Implementation Date	Manager Responsible
2.1	Management need to ensure that at least 95% of all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual IG training before the 31st March 2018 deadline.	Low	Y	IG Training compliance is now at 94.2%. There is a further training session on Wednesday 28th March and staff are continuing to update their training on line. A final report will be taken on Wednesday afternoon following the training. It is expected that the training will achieve 95% compliance rate on this date	28/03/2018	Tracey O'Mullane

Appendix A

Findings and Recommendations

This report has been produced by exception. Therefore, we have included in this section only those areas of weakness in control or failure to apply controls identified from our testing and not the outcome of all testing undertaken. Management action prioritisation is detailed at Appendix B.

Requirement 14.1 -112: Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained.					
Ref	**Control**	**Adequate (Y/N)**	**Test result and / or implication**	**Recommendation**	**Priority**
2.1	**Level 2a:** At least 95% of all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual IG training in the period 1 April to 31 March. For NHS organisations - staff will have been trained at least once using the online materials in the NHS IGTT (e-learning or trainer presentations). In subsequent years, training can be provided using locally approved materials.	N	As at 16th March 2018, 91% of staff had completed their annual IG training. The Trust must train a further 4% of staff to reach the 95% training target. This presents a risk that the Trust will not meet level 2a of the requirement which will result in an unsatisfactory annual toolkit submission.	Management need to ensure that at least 95% of all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation have completed their annual IG training before the 31st March 2018 deadline.	Low

Appendix B

Recommendation Prioritisation

Recommendation Prioritisation	
High	A fundamental weakness in the system that puts the achievement of the systems objectives at risk and / or major and consistent non-compliance with the control framework requiring management action as a matter of urgency.
Medium	A significant weakness within the system that leaves some of the systems objectives at risk and / or some non-compliance with the control framework.
Low	Minor improvement to the system could be made to improve internal control in general and engender good practice but are not vital to the overall system of internal control.