INTERNAL AUDIT REPORT

2016/17

Review of the Information Governance Toolkit

Index:

Executive Summary

Background-General

Information Governance allows organisations and individuals to ensure that personal information is handled legally, securely, efficiently and effectively, in order to deliver the best possible service.

The Information Governance Toolkit is an online system which allows NHS organisations and other providers of NHS commissioned services to assess themselves against the Department of Health's Information Governance policies and standards. It also allows members of the public to view participating organisations' Information Governance toolkit assessments.

The toolkit assesses Information Governance management, confidentiality and data protection assurance, information security assurance and clinical information assurance.

It is a requirement of the NHS England contract that all providers complete and submit, on an annual basis, the Information Governance toolkit. The work involves a self-assessment of compliance against the IG requirements. There are 3 levels of self-assessment, from level 1 (planning), level 2 (doing) and level 3 (check and acting upon). The NHS England contract requires a level 2 attainment.

A requirement of the NHS England contract is that an audit is undertaken on the Information Governance Toolkit submission, with the audit report included not only with the final submission, but included on the organisation's website.

Background -Our Compliance

We have completed and submitted the NHS Information Governance toolkit for a number of years. This involves a self-assessment and we have self-assessed ourselves at level 2.

We sought clarification from NHS England in 2015 on the appropriate arrangements we should adopt for this audit, given the Compliance & Audit Manager completes the Information Governance toolkit and therefore could not undertake an audit on the submission. NHS England confirmed that a person working at our Charity could complete the audit, as long as they are independent of our work on Information Governance and the completion of the toolkit.

The audit on the 2016/17 Information Governance toolkit has therefore been undertaken by the Change Delivery & Improvement Adviser.

Scope and Objectives

We reviewed the overall reasonableness of the submission responses to all the questions asked. In addition we reviewed in particular the adequacy of the responses and supporting documentation for:

- Section 115–There is an information governance policy that addresses the overall requirements of information governance;

- Section 117-All staff members are provided with appropriate training on information governance requirements;

- Section 317–Unauthorised access to the premises, equipment, records and other assets is prevented; and

- Section 325–Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely.

Overall Conclusion

The overall conclusions in this report are that the responses and the self-assessment scores of 2 in the Information Governance toolkit are adequately supported by appropriate evidence.

There were five low risk recommendations made in this report, which do not impact upon the overall self-assessment scores of 2.

Recommendations

Our recommendations are detailed in the body of this report and are also shown in an action plan in Appendix A to this report.

In Appendix A we have graded the recommendations according to risk and we obtained agreement for responsibility for implementing them, alongside an agreed timescale.

Way forward

We discussed and agreed the recommendation with our colleagues and have issued this report as a final document, which will go to the Audit Committee (and DMT for information).

We will undertake a follow up to assess progress made in implementing the recommendation from this report in 2017/18.

We would like to formally acknowledge the help of staff in the completion of this audit.

Detailed Report

Overall review

We reviewed the submission for all sub-sections within the Information Governance toolkit for reasonableness and there are no matters of concern to highlight in this audit report.

Section115–There is an information governance policy that addresses the overall requirements of information governance

We reviewed the comments and supporting evidence for section 115 of the Information Governance toolkit. There was appropriate supporting evidence for a level 2 self-assessment. However, it was noted that although we have an Information Governance policy, it needs updating to fully reflect our current Information Governance arrangements.

R1 The Information Governance policy is updated.

Section 117-All staff members are provided with appropriate training on information governance requirements

We reviewed the comments and supporting evidence for section 117 of the Information Governance toolkit. There was appropriate supporting evidence for a level 2 self-assessment. The level of completion of the mandatory Information Governance on-line course by staff has reduced from the very high levels in 2015/16. The Learning & Development Team stated this was predominantly a reflection of staff not renewing the completion of this course on an annual basis, rather than new staff not completing the course at the start of their career with us. The Learning & Development Team are looking to refresh the Information Governance on-line course. It is appropriate for line-managers to monitor completion of this mandatory course for all staff they line-manage.

R2 Completion of the mandatory on-line IG course is made an objective for all staff, which all line managers robustly monitor.

Section 317–Unauthorised access to the premises, equipment, records and other assets is prevented

We reviewed the comments and supporting evidence for section 317 of the Information Governance toolkit. There was appropriate supporting evidence for a level 2 self-assessment. The Charity's business continuity plan was tested in 2016.

R3 The Business Continuity Plan testing undertaken in 2016 is built upon.

Section 325–Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely

We reviewed the comments and supporting evidence for section 325 of the Information Governance toolkit. There was appropriate supporting evidence for a level 2 self-assessment. The Head of IT is overseeing our-self assessment against the 'Cyber Essentials' scheme and is also planning to ensure an external organisation undertakes the annual IT penetration tests on our computer systems. It will be useful to communicate the results of both pieces of work to our Audit Committee.

R4 The results of the self-assessment against 'Cyber Essentials' and the third party IT penetration tests are reported to our Audit Committee.

Recommendation from the 2015/16 Information Governance toolkit Internal Audit Report: **Prior year audit recommendation**: A Data Protection Policy has been updated and is available to all staff on the organisation's Intranet. We need to ensure the policy is fully embedded within the organisation, including incorporation into existing data protection induction materials.

Appendix A- Action Plan

Recommendation	Risk Category (determined by the impact and likelihood of the risk)	Agreed/Not Agreed?	Additional comments	Date for implementation	Responsible Officer
R1 The Information Governance policy is updated.	Low	Agreed	It is acknowledged that the current policy requires review.	31 December 2017	Director of Legal & Corporate Governance
R2 Completion of the mandatory on-line IG course is made an objective for all staff, which all line managers robustly monitor.	Low	Agreed	Whilst completion will be managed individually through goals and learning requirements by role. An exception report will be circulated to the Directors' Management Team to ensure full compliance.	31 January 2018	Director of People & OD
R3 The Business Continuity Plan testing undertaken in 2016 is built upon.	Low	Agreed	The Business Continuity (BC) team in Northampton have held roundtable discussions about local BC procedures with all regional offices and these are reviewed in accordance with	31 December 2017	Director of Finance & Resources until Head of Facilities appointed.

			the BC schedule. Further testing will be planned in accordance with the overall BC plan.		
R4 The results of the self-assessment against 'Cyber Essentials' and the third party IT penetration tests are reported to our Audit Committee.	Low	Agreed	No comments to make.	March and/or June 2017 Audit Committee	Head of IT
Prior year audit recommendation: A Data Protection Policy has been updated and is available to all staff on the organisation's Intranet. We need to ensure the policy is fully embedded within the organisation, including incorporation into existing data protection induction materials.	Low	Agreed	The policy was communicated to staff through our internal communications team during 2016. Further communications will be generated to provide a consistent message and to also ensure managers embed policy and requirements within their teams.	31 December 2017	Director of Legal & Corporate Governance