BLACKPOOL CLINICAL COMMISSIONING GROUP

ANNUAL REPORT TO THE SENIOR INFORMATION RISK OWNER

MARCH 2015

INTRODUCTION

Every year the CCG must demonstrate compliance with Information Governance requirements by completing the Health & Social Care Information Centre IG Toolkit. There is a requirement for all NHS organisations to meet the minimum of level 2 across ALL requirements within the toolkit. However year on year the CCG should also seek to improve this score and show that the IG work programme is embedded within the organisation and continually reviewed to ensure IG requirements meet the needs of the organisation.

IG TOOLKIT SUBMISSION

On the 31st March the CCG will submit the Information Governance Toolkit return following approval and the Finance and Performance Committee on 24 March 2015. The 2014-15 submission for Blackpool CCG is:

Information Governance Management

Assessment Period	Level						Outcome
	0	1	2	3	N/R	Exempt	Score & Status
Version 12 (2014-2015)				**5**			**100%**

Confidentiality and Data Protection Assurance

Assessment Period	Level						Outcome
	0	1	2	3	N/R	Exempt	Score & Status
Version 12 (2014-2015)			**4**	**3**	**1**		**80%**

Information Security Assurance							
Assessment Period	**Level**						**Outcome**
	0	1	2	3	N/R	Exempt	Score & Status
Version 12 (2014-2015)			**5**	**5**	**3**		**83%**

Clinical Information Assurance							
Assessment Period	**Level**						**Outcome**
	0	1	2	3	N/R	Exempt	Score & Status
Version 12 (2014-2015)			**1**	**1**			**83%**

Overall Submission							
Assessment Period	**Level**						**Outcome**
	0	1	2	3	N/R	Exempt	Score & Status
Version 12 (2014-2015)			**10**	**14**	**4**		**86%**

INFORMATION GOVERNANCE POLICIES AND PROCEDURES

The CCG has continued with the IG Policy and Handbook approved in January 2014 for this IG Toolkit year. Both documents are due for ratification in 2015/16. The CCG IG Leads and CSU IG Team will agree the approach for reviewing the existing Policy and Handbook at the beginning of the 2015/16 financial year.

INFORMATION GOVERNANCE IMPROVEMENT PLAN

The Information Governance Improvement Plan has been reviewed within the year and the CCG is now in a position where all actions within the plan that relate to the submission of the IG Toolkit have been completed.

For the forthcoming year, an improvement plan will be developed and implemented to further reinforce the CCGs compliance with the IG toolkit requirements, with particular focus on:

- Developing closer working links with the CCGs SIRO and Caldicott Guardian and ensuring their active involvement in the IG agenda.

- Development and implementation of an integrated online system to support the Information Risk Assessment and Management Programme with the aim of strengthening the data collected about the CCGs Information Assets and Data Flows, and ensuring there are adequate supplier/sharing partner contracts/agreements and back-up/disaster recovery/business continuity plans in place where required.

- Further developing the IG training programme to move towards ensuring staff understand how to apply IG to their day to day working, rather than simply having an awareness of IG principles.

- Improving the records management standards implemented within the CCG.

STAFF UNDERSTANDING OF INFORMATION GOVERNANCE

It is an annual requirement for all staff employed by the CCG to undertake Information Governance training. This year, refresher training was provided through face to face sessions facilitated by the CSU IG team using training materials that had been externally audited and found to be "more comprehensive and benefit from additional content" when compared to the equivalent modules on the HSCIC IG Training Tool.

As part of this refresher training, staff were asked to complete an interactive assessment throughout the session through the use of voting devices. While anonymous during the session, the data captured allowed the IG team to identify the responses given by each candidate and therefore fulfil the requirement for staff to have completed an assessment of their understanding.

Staff who were unable to attend one of the face to face training sessions were asked to complete their IG training by completing the refresher module on the IG Training Tool.

Overall 100% of staff employed by the CCG completed their IG training during 2014/15.

In addition to the mandatory IG training, staff understanding of local IG policy and procedures was tested as part of the Working Hours Information Security Spot Checks carried out on CCG premises. A sample of staff were asked several questions regarding local IG arrangements and reflecting the content of the face to face refresher training sessions. The outcomes of these checks show that levels of staff understanding of local IG arrangements and basic IG principles are generally very good within the CCG.

This is not however a subject area with which we should become complacent especially as the landscape of IG is changing on frequent basis.

SUBJECT ACCESS REQUESTS

Between 1st April 2014 and 31st March 2015, the CCG has received no data protection requests.

This has been confirmed by the Subject Access Lead for the CCG. All staff with responsibility for the management of subject access requests do however remain up to date with the associated training and have procedures to follow should they receive a request.

CALDICOTT ISSUES

The recommendations of the Caldicott Committee (1997 Caldicott Report) defined the confidentiality agenda for NHS organisations. A key recommendation was the appointment in each NHS Trust and special health authority (e.g. NHS Business Services Authority) of a "Guardian" of patient identifiable information to oversee the arrangements for the use and sharing of patient information.

The Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. They are a 'conscience' of an organisation.

The Caldicott Guardian works closely with the CSU IG Team completing a 'Caldicott Issues Log' when an issue and/or decision are required by the Caldicott Guardian.

INFORMATION RISK MANAGEMENT AND ASSURANCE

The 2014-15 Information Risk Assessment and Management Programme is set out in the CCGs IG Improvement Plan.

Within the year the CCG has reviewed the Information Asset Owners and Administrators to ensure that all work areas within the organisation have appropriate cover.

The Senior Information Risk Owner has completed training to ensure they are suitably equipped for their role.

The work completed by IAAs and IAOs, with the support of the CSU IG team, during 2014-15 has covered:

- ✓ Identification and recording of information asset s
- ✓ Risk assessment of how each asset is held
- ✓ Identification of associated data flows
- ✓ Risk assessment of the data flows
- ✓ Business Impact Assessment for each of the assets

INFORMATION ASSET REGISTER

The CCGs Information Asset Register contains details of 97 information assets. Of these, 26 have been identified as containing person confidential data. Each asset has been risk assessed according to the information provided in the asset register describing the information contained within the asset and how the asset is held. No assets were found to have a risk score of 12 or more.

BUSINESS CRITICAL ASSETS

A business impact assessment has been carried out for each recorded asset to allow business critical assets to be identified. An asset is defined as being business critical if the impact of it being unavailable for 3 days (in the worst case scenario, e.g. during the period at which the asset is most accessed) is assessed at a score of 3 or higher (on a scale of 1 to 5).

The assets that have been identified as being business critical to the CCG are included in **Appendix A** of this report.

2 paper based critical assets currently don't have a business continuity plan in place. The SIRO has been informed of this and the IG team will meet with the IAO to discuss the options to mitigate this.

DATA FLOW MAPPING

For those assets that were identified as containing person confidential data or business sensitive information, it is necessary to identify if the asset is received from or sent to anywhere outside of the team responsible for the asset. If this was found to be the case, a data flow mapping questionnaire was completed.

51 assets have been identified as having an associated data flow. Any data flows which occur on an ad hoc basis were recorded but no further information regarding the methods of transmission were recorded as the IG toolkit specifically indicates that this is not necessary.

It is expected that as the work programme continues, more data flows will be mapped and associated risks managed as required.

INFORMATION GOVERNANCE INCIDENTS

All serious data breaches assessed at level 2 or more are reported to the SIRO and support is provided by the IG team within the CSU in the investigation and management of the incidents. Between the 1st April 2014 and 31st March 2015 there have been no level 2 IG incidents reported.

PRIVACY IMPACT ASSESSMENTS

All new projects, processes and systems (including software and hardware) which are introduced must comply with confidentiality, privacy and data protection requirements. A Privacy Impact Assessment (PIA) is a tool which can help the CCG identify the most effective way to comply with these requirements and to fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

It is the CCGs responsibility to ensure that for any services they commission where person confidential data is to be used in any way, that a Privacy Impact Assessment is carried out to provide assurance to the Data Controllers and Data Processors involved in the provision of the service that the service is compliant with the requirements of privacy law. It is therefore imperative that a PIA is competed during the planning of any new projects, processes or systems under consideration by the CCG which involve the use of person confidential data in any way.

This requirement is highlighted to all CCG staff through the Information Governance Refresher Training.

During 2014/15 a total of 2 PIAs were completed for consideration. All PIAs were approved by IG and didn't require any changes to be made to the project to which they related.

INFORMATION SECURITY SPOT CHECKS

All work areas within the CCG have been subject to Information Security Spot Checks. These checks were unscheduled and have been carried out both within and outside working hours to review compliance with the CCGs procedures and whether staff are adhering to them in their day to day working. The focus of the checks therefore varied dependent upon the time of the audit as some aspects, such as clear screen, are not applicable outside of working hours.

OUT OF HOURS

The spot check took place on 30 January 2015 at the end of the working day. Whilst there were some excellent examples of clear desk policies especially to note in Admin, CSU, Choose & Book, Ambulance Commissioning and Finance there were a number of staff who didn't comply with the standards. Below is a list of areas where compliance was not in place:

- 2 laptops left out from the previous working day
- Large volumes of paperwork left on desks, some of which considered commercially sensitive
- 3 filing cabinets containing patient records left open with keys left inside the locks

This has been raised with the SIRO, who will ensure colleagues are made aware and follow CCG procedures.

WORKING HOURS

The spot check took place on 13 February 2015 during the working day. All areas audited were compliant with working hour standards apart from 2 areas. It was noted on several occasions that some staff members left their desks to go out of the office without locking their computer screens. Some staff member's desks contained large volumes of paperwork. This has been included within the IG training sessions.

During the audit, 3 members of CCG and 2 embedded CSU members of staff were interviewed at random to audit their knowledge and understanding to Information Governance within the CCG. To highlight the 3 CCG staff interviewed, whilst demonstrating excellent understanding of IG within most areas, there was confusion of who was the IG Lead for the CCG.

INFORMATION SECURITY AND CONFIDENTIALITY AUDIT OUTCOMES

In addition to the spot checks, an Information Security Audit and a Confidentiality Audit has also been carried out within the CCG. The purpose of the Information Security Audit was to test the information collected in the Information Asset Register regarding the security arrangements in place to protect physical (in particular paper) assets. It was found that the physical assets selected for audit were found to be correct as stated within the information asset register.

The majority of the physical assets audited were found to have excellent practices in place including tracking procedures when part of the asset is removed.

The Confidentiality Audit focussed on the access controls in place to protect information assets held electronically on the CCGs shared drive, in terms of ensuring that the access groups are correctly populated. 5 electronic assets containing personal confidential data were selected at random. Each IAO/IAA was asked which staff members should have access to the asset. This was then compared via a request to IT. It was found that 2 out of 5 assets didn't match. The IAO/IAA for each asset has been informed of the discrepancies and an action plan is in place to work with the IAO/IAA to resolve the discrepancies.

APPENDIX A – BUSINESS CRITICAL ASSETS

Asset Name	Team	IAO	What information is contained in the asset?	Asset Format	Asset Risk Score	Is there a business continuity plan in place which covers this asset?	What would be the impact to the organisation, patients or legal/contractual implications of this asset being unavailable for 3 days (worst case scenario)
Journals	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Noticeable impact but no major impact on the business or to personnel
Budget Adjustments	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Noticeable impact but no major impact on the business or to personnel
Trial Balance	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Noticeable impact but no major impact on the business or to personnel
Working Papers	Finance	Clare Cosgrove	Financial Information – Budget/Contracting	Electronic	4	Yes	Noticeable impact but no major impact on

Asset Name	Team	IAO	What information is contained in the asset?	Asset Format	Asset Risk Score	Is there a business continuity plan in place which covers this asset?	What would be the impact to the organisation, patients or legal/contractual implications of this asset being unavailable for 3 days (worst case scenario)
			Information				the business or to personnel
Cash Requests	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Noticeable impact but no major impact on the business or to personnel
Cash Forecasts	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Noticeable impact but no major impact on the business or to personnel
Finance Reports	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Noticeable impact but no major impact on the business or to personnel
Planning Templates	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Considerable impact on resources, personnel or costs
Budget Setting Papers	Finance	Clare Cosgrove	Financial Information – Budget/Contracting	Electronic	4	Yes	Considerable impact on resources,

Asset Name	Team	IAO	What information is contained in the asset?	Asset Format	Asset Risk Score	Is there a business continuity plan in place which covers this asset?	What would be the impact to the organisation, patients or legal/contractual implications of this asset being unavailable for 3 days (worst case scenario)
			Information				personnel or costs
Annual Accounts Templates	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Considerable impact on resources, personnel or costs
Annual Accounts Working Papers	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Considerable impact on resources, personnel or costs
Non ISFE templates	Finance	Clare Cosgrove	Financial Information – Budget/Contracting Information	Electronic	4	Yes	Considerable impact on resources, personnel or costs
Pay Working Papers	Finance	Clare Cosgrove	Financial Information – Staff Information	Electronic	5	Yes	Noticeable impact but no major impact on the business or to personnel
Resource Library	Ambulance Commissioning	Allan Jude	Correspondence – Other	Electronic	3	Yes	Considerable impact on resources, personnel or costs
Provider Contracts	Ambulance Commissioning	Allan Jude	Contracts or Agreements	Electronic	4	Yes	Considerable impact on resources,

Asset Name	Team	IAO	What information is contained in the asset?	Asset Format	Asset Risk Score	Is there a business continuity plan in place which covers this asset?	What would be the impact to the organisation, patients or legal/contractual implications of this asset being unavailable for 3 days (worst case scenario)
							personnel or costs
Ambulance Commissioning Letters and Correspondence	Ambulance Commissioning	Allan Jude	Correspondence – Other	Electronic	3	Yes	Considerable impact on resources, personnel or costs
Complaints	Ambulance Commissioning	Allan Jude	Correspondence - Complaints	Electronic	5	Yes	Considerable impact on resources, personnel or costs
Performance & Finance Reports	Ambulance Commissioning	Allan Jude	Correspondence – Financial/Contracting	Electronic	4	Yes	Considerable impact on resources, personnel or costs
FOI Requests	Ambulance Commissioning	Allan Jude	Correspondence – Legal Requirements	Electronic	2	Yes	Considerable impact on resources, personnel or costs
Patient Assessments (Archive)	Continuing Healthcare	Alison Small	Patient/Service User Records	Paper	5	No	Noticeable impact but no major impact on the business or to personnel
Patient	Continuing	Alison Small	Patient/Service User	Electronic	5	Yes	Considerable impact

Asset Name	Team	IAO	What information is contained in the asset?	Asset Format	Asset Risk Score	Is there a business continuity plan in place which covers this asset?	What would be the impact to the organisation, patients or legal/contractual implications of this asset being unavailable for 3 days (worst case scenario)
Assessments	Healthcare		Records				on resources, personnel or costs
Patient Assessments	Continuing Healthcare	Alison Small	Patient/Service User Records	Paper	5	No	Considerable impact on resources, personnel or costs
Choose & Book Team Folders	Choose & Book	Steve Gornall	Staff Personnel Records	Electronic	5	Yes	Noticeable impact but no major impact on the business or to personnel
Choose & Book Training Materials	Choose & Book	Steve Gornall	Training Materials	Electronic	1	Yes	Considerable impact on resources, personnel or costs
Choose & Book Information Requests	Choose & Book	Steve Gornall	Correspondence – Patient Information	Electronic	5	Yes	Business threatening or likely to attract national media coverage, legal action or serious financial penalty

Asset Name	Team	IAO	What information is contained in the asset?	Asset Format	Asset Risk Score	Is there a business continuity plan in place which covers this asset?	What would be the impact to the organisation, patients or legal/contractual implications of this asset being unavailable for 3 days (worst case scenario)
Provider Meeting Documentation	Ambulance Commissioning	Allan Jude	Meeting Documents – Financial/Contracting	Electronic	4	Yes	Considerable impact on resources, personnel or costs