South West London
Merton Clinical Commissioning Group

Report to the Merton Clinical Commissioning Group Governing Body

Date of Meeting: Thursday 21st March 2013

Agenda No: 7.5 **ATTACHMENT 14**

Title of Document: Merton CCG Information Governance Assessment 2012-2013	**Purpose of Report:** To Receive and Note
Report Author: Glyn Jones, Information Governance Manager - CSU	**Lead Director:** Karen McKinley, CFO

Contact details: glyn.jones@swlondon.nhs.uk

Executive Summary:
The MCCG is required to make a baseline self assessment against the CfH Information Governance Toolkit version 10. The attached document is a summary of the IG Toolkit base line assessment which will be made before the 31st March 2013.

On the basis of the current implementation and supporting evidence the CCG is 24.7% compliant against the 28 CCG requirements.
An improvement plan will be developed to achieve the required level 2 compliance, by 31st March 2014', thereby achieving the 66.7% overall target score.

The improvement plan will be actively monitored by the Merton Clinical Executive Team and facilitated by the CSU IG Manager on a monthly basis.

Non compliance poses a number of risks to the CCG which if not mitigated could lead in a significant data loss or breach and result in a financial penalty and loss of professional reputation. IG risks must be identified on the risk register, monitored by the Executive Team and reviewed by the MCCG Governing Body.

Key sections for particular note (paragraph/page), areas of concern etc:
The risk to the CCG of non-compliance has been scored as a 12 (Amber). The consequence for the CCG will be:

- It does not achieve the 'trusted' organisation status needed to make information sharing easier between stakeholders and partners.
- It may be seen as contributory factor in any subsequent ICO investigation, if a significant data loss occurs.
- That without a realistic improvement plan the retention of the N3 connection may be in jeopardy.

Recommendation(s):
The Merton Clinical Commissioning Group Governing Body is requested to:
1. Accept the self assessment and score which will be made by the end of March 2013
2. Acknowledge that non-compliance represents an information risk to the CCG, which must be identified and managed through the Board Assurance Framework.
3. Provide a clear commitment to the achievement of level 2 compliance by March 2014 as the key method of mitigating the risks identified.

Committees which have previously discussed/agreed the report:
The Clinical Executive Team

Financial Implications:
None, unless alternative or additional resource is needed to meet requirements**.**

Implications for the Sutton and Merton Board or Joint PCT Boards:
The input to meeting CCG IG compliance will support NHS SW London and nominated SIRO to manage information risks until the end of March 2013.

Other Implications: (including patient and public involvement/Legal/Governance/ Risk/ Diversity/ Staffing) Non-compliance may result in the CCG not meeting legislative and good practice requirements. IG compliance is about providing assurances to the Board, stakeholders and patients and is seen as essential in its legal role as 'Data Controller, under the Data Protection Act 1998.
Equality Analysis: The IG work plan will ensure equality in the implementation process. Staff will be given equal access to all guidance and training, with all staff expected to understand their responsibilities and requirements.
Information Privacy Issues: The Data Protection Act 1998 places a legal responsibility on all organisations. A significant breach could result in a financial penalty and loss of professional reputation.
Communication Plan: (including any implications under the Freedom of Information Act or NHS Constitution) Communications for the staff will be developed through the Clinical Executive Team. All IG material will be available in response to FOI requests, unless exemptions are applicable. The following information must be made available to staff and the public through the MCCG intranet and the Publication Scheme: • Fair Processing Notice • Subject Access Request Policy • IG related Policies and Guidance

South West London

Merton Clinical Commissioning Group

Merton Clinical Commissioning Group Information Governance Assessment

2012-13 – .Summary Report

1.1 The March 31st 2013 baseline assessment against version 10 of the IG Toolkit will be formally submitted before the end of March. This will show that based on current implementation and supporting evidence the CCG scored **24.7 %,** against the required standards. There is no expectation that the CCG as a 'shadow' organisation can meet IG requirements by the end of March. The assessment reflects a situation where most of the compliance evidence available was generated to meet the IG compliance needs of the NHS SW London Cluster and will need to be re-evaluated for use by the CCG. This will not be achieved before the end of March.

1.2 The requirement now is that the CCG should achieve a minimum of level 2 compliance against each of the 28 standards by 31st March 2014. The target Level 2 compliance would provide a score of **66.7%**

1.3 The Table 1 below provides a summary against each of the IG Toolkits main initiatives.
Table 1

INITIATIVE	Assessment Requirements	Baseline Assessment % Score 31.03.13
Information Governance Management	5	40.0
Confidentiality and Data Protection	8	28.6
Information Security Assurance	13	17.9
Clinical Information Assurance	2	16.7
Total	**28**	**24.7**

1.4 The requirement will now be to develop an improvement plan which addresses the gaps and for this to be actively managed and monitored by the Clinical Executive Team. The IG Toolkit is a self assessment process, which requires supporting evidence to confirm the stated score. It will be a requirement for the self assessment to be independently audited as part of the CCG's internal audit programme, to validate the stated compliance score.

Risk to Cluster of Non Compliance

1.5 The risk of IG Toolkit non-compliance has been assessed as a score of 12 AMBER). The risks associated with continued non-compliance are:

- not having 'trusted organisation status' (achieved by scoring level 2for all standards) which enables the automatic sharing of PID between partner organisations without specific agreements
- failure to meet IG standards may be seen as contributory factor in any subsequent ICO investigation, if a significant data loss occurs.
- where the IG Toolkit standards are not met to an appropriate standard (Minimum level 2), an action plan for making the necessary improvements must be agreed with the Department of Health Information Governance Policy team or with an alternative body designated by the Department of Health (e.g. a commissioning organisation) to maintain the N3 connection

1.6 There are a number of specific IG risks which are related to not meeting the achievement of level 2 for individual standards. These risks have been identified and will be managed as part of the Board Assurance Framework. IG related risks will be included on the risk register, monitored by the Executive Team and Reviewed by the MCCG Governing Body.

IG Next Steps

1.7 The emphasis for the CCG acting in shadow mode has been to establish an IG management framework with the key roles of IG Lead, SIRO and Caldicott Guardian identified. The work to continue to embed this into the organisation is essential.

1.8 Almost 50% of the requirements fall into the Information Security Assurance category, therefore evidence of compliance will need to be provided by the CSU Informatics function.

1.9 The immediate key risks identified are those posed as a result of the transition and relate to the transfer of information assets to successor organisations. There is a need to identify:

- Which organisation are 'data controllers' and which are 'data processors'
- The legal basis for using and sharing data (being determined nationally)
- The need for contractual processing agreements with all third parties
- And map inbound and outbound data flows
- All information assets and Information Asset Owners (IAO)
- IG training requirements

Glyn Jones

Information Governance Manager

NHS SW London

Version 0.2

12.03.13

Information Governance Toolkit Workbook (Version 10) -
Clinical Commissioning Groups
Merton CCG
Requirement List

Req No	Description	Past Level	Current Level	Target Level
Information Governance Management				
10-130	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda		**1**	**2**
10-131	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans		**1**	**2**
10-132	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations		**1**	**2**
10-133	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation		**1**	**2**
10-134	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained		**2**	**2**
Confidentiality and Data Protection Assurance				
10-230	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs		**1**	**2**
10-231	Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users		**1**	**2**

10-232	Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected		**1**	**2**
10-233	Individuals are informed about the proposed uses of their personal information		**1**	**2**
10-234	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data		**1**	**2**
10-235	There are appropriate confidentiality audit procedures to monitor access to confidential personal information		**0**	**2**
10-236	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines			**NA**
10-237	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		**1**	**2**
Information Security Assurance				
10-340	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs		**1**	**2**
10-341	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed		**0**	**2**
10-342	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority		**1**	**2**
10-343	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use		**1**	**2**

10-344	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		**1**	**2**
10-345	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy		**1**	**2**
10-346	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		**0**	**2**
10-347	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely		**1**	**2**
10-348	Policy and procedures ensure that mobile computing and teleworking are secure		**1**	**2**
10-349	There are documented incident management and reporting procedures		**1**	**2**
10-350	All transfers of hardcopy and digital personal and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers		**0**	**2**
10-351	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures		**0**	**2**
10-352	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate		**0**	**2**
Clinical Information Assurance				
10-420	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience		**1**	**2**
10-421	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements		**0**	**2**