NHS DORSET CLINICAL COMMISSIONING GROUP

GOVERNING BODY

INFORMATION GOVERNANCE TOOLKIT REPORT

Date of the meeting	20/07/2016
Author	J Green, Head of Information Governance/Customer Care
Sponsoring Clinician	Dr J Bubb, Locality Chair for Mid Dorset
Purpose of Report	To assure the Governing Body that the requirements of the Information Governance Toolkit are being met and that significant improvements continue to be made across the CCG.
Recommendation	The Governing Body is asked to **note** the report.
Stakeholder Engagement	N/A
Previous GB / Committee/s, Dates	N/A

Monitoring and Assurance Summary

This report links to the following Assurance Domains	- Services designed around people - Preventing ill health and reducing inequalities - Sustainable healthcare services - Care closer to home		
I confirm that I have considered the implications of this report on each of the matters below, as indicated:	**Yes** [e.g. ✓]	**Any action required?**	
		Yes Detail in report	**No**
All three Domains of Quality (Safety, Quality, Patient Experience)	✓		✓
Board Assurance Framework / Risk Register	✓		✓
Budgetary Impact	✓		✓
Legal / Regulatory	✓		✓
People / Staff	✓		✓
Financial / Value for Money / Sustainability	✓		✓
Information Management &Technology	✓		✓
Equality Impact Assessment	✓		✓
I confirm that I have considered the implications of this report on each of the matters above, as indicated	✓		

Initials: JG

1.   Introduction

1.1   Every year the CCG must demonstrate compliance with Information Governance (IG) requirements by completing the Information Governance Toolkit (IGT).

1.2   Effective IG is critical as the loss, or inappropriate disclosure of personal information, can cause significant distress to patients and staff, undermine trust in the organisation and lead to fines of up to £500,000.

1.3   The IGT is the Department of Health's policy delivery vehicle that the Health and Social Care Information Centre (HSCIC) is commissioned to develop and maintain.

1.4   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.

1.5   In accordance with the requirements of the IGT, the purpose of this report is to provide the Governing Body with assurances in relation to IG management and accountability, advise of any level 2 IG incidents, and provide an update in respect of the IGT assessment.

1.6   The IGT performance results are freely available and provide assurance of the CCG's performance in looking after personal information to regulatory bodies, stakeholders and the general public. The results are also required to be published in the CCG's Annual Report.

1.7   As a commissioner we are required to monitor the Information Governance performance of providers to support the recommendations of the Francis Report and so reduce risk.

2.   Information Governance

Information Governance Internal Accountability/Responsibility

2.1   The Information Governance Group (IGG) met on a bi-monthly basis during 2015/16. The group is chaired by the Senior Information Risk Owner (SIRO) and is attended by the Caldicott Guardian, Head of Information Governance and Customer Care, the Senior Audit Manager and representatives from each directorate. The group reports via the Audit and Quality Committee.

2.2   The IGG has overseen the work plan for the CCG during 2015/16, in relation to the IGT and the development and approval of core IG framework policies and procedures.

2.3   It is essential to ensure that the Governing Body and the senior management of the organisation are assured of continued compliance, and in particular, changes in performance both within the CCG and commissioned services.

IG Toolkit Assessment 2015/16

2.4   The IGT requires CCGs to complete a self-assessment against four initiative sets:

- Information Governance Management;

- Confidentiality and Data Protection Assurance;

- Information Security Assurance;

- Clinical Information Assurance.

and 28 key requirements (see appendix 1). A full assessment is required to be submitted no later than 31 March 2016. This requires uploading the evidence of compliance against the key factors in order to obtain a score.

2.5   The toolkit enables the CCG to measure its performance through an annual self-assessment audit process and report upon levels of compliance against a set number of requirements.

2.6   Organisations are required to achieve a final overall score of "Satisfactory" which means that all requirements must be assessed at level 2 or above. This is regardless of the amount of progress made against each of the individual requirements.

2.7   The IGG verified the submission of version 13 of the 2015/16 IGT and the score as 71%, satisfactory.

2.8   The submission for 2015/16 took place in March 2016. The CCG achieved an overall score of 'Satisfactory' with 24 criteria at level 2 and 4 criteria at level 3. See appendix 2.

Audit Findings

2.9   Prior to submitting its final assessment, the CCG's internal auditors, TIAA audited a sample of 10 requirements and attended an IG Training session. A substantial assurance opinion was issued as follows "the CCG has provided sufficient evidence to support its self-assessed scores and no recommendations are required".

2.10 The Governing Body can take assurance that the controls upon which the organisation relies to manage IG are consistently applied and effective.

Information Governance Training

2.11   In order to comply with requirement 13-14 of the IGT:

- staff attendance at the training is mandatory and has to be repeated annually;

- there must be staff attendance of no less than 95%.

In 2015/16 Dorset CCG achieved 100% of staff attending. This has been verified by Workforce.

2.12   In total eighteen face to face training sessions took place between September 2015 and February 2016. All sessions were well attended and staff feedback indicates that they enjoyed the training and felt it increased their understanding of IG within their role.

2.13   Unlike other mandatory training within the NHS the IG Training does not run on a rolling 12-month cycle. The training year is from the 1 April to the 31 March. For this reason, on the 1 April, all training records are returned back to 0% noncompliant. This is set nationally by the HSCIC.

2.14   Dates for mandatory IG Training for 2016/17 have been issued. Training material is being revised to ensure currency.

IG 'Spot Checks'

2.15   The IG and IT Teams are currently working together to improve security of personal information, both paper and electronic, within the CCG. 'Spot checks' have been introduced both during working hours and out of hours. Reports are to be provided to the SIRO and the IGG.

2.16   Regular reminders are sent to staff regarding the importance of locking screens and ensuring documents are not left out on desks unattended during the working day and out of hours. These are followed up verbally and via the staff bulletin.

Policies and Procedures

2.17   The IG Policies have been updated and amalgamated into one policy. This was discussed and approved at the IGG on 16 December 2015 and Directors on 16 February 2016. The policy is available to staff on the CCG Intranet and to the public on the Dorset CCG Website.

Confidentiality: Staff Code of Conduct Handbook

2.18   The IGT requires a number of different policies and procedures as evidence to support the submission, one of which is a staff handbook. This has been revised. The following areas are included within the revised handbook:

Basic Principles of IG;	IG Legal Framework;
Access to Personal Information;	Sharing of Information;
Caldicott Principles;	Privacy Impact assessments;
Information Assets;	Confidentiality Audits;
Home Working;	Freedom of Information;
Subject Access Procedure;	Privacy Impact Assessments;
Information Security;	Mobile Media;
Confidentiality and Data Protection;	
Confidentiality Breaches/Incident Reporting.	

2.19   All staff receive a booklet during their Induction Training and revisions have been notified to other staff.

Privacy Impact Assessments (PIA)

2.20   It is essential that the IG team is informed of the planning of any new services, processes or systems in order to ensure a PIA is completed. This is a requirement of the IGT and also the independent body who oversees the provisions of the Data Protection Act. Use of PIAs is also due to become law in 2018.

Privacy Notice (Fair Processing)

2.21   This is a requirement which informs individuals how their personal information is used by the CCG. It is accessible from the CCG's website and also in a booklet which can be given to an individual.

Serious Untoward Incidents

2.22   The CCG had no serious untoward incidents in relation to IG.

Information Commissioner Notices

2.23   Dorset CCG has not been subject to any Information Commissioner data protection monetary penalties.

Compliance with Legal and Regulatory Framework

2.24   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.

Freedom of Information

2.25   The CCG received 318 FOI requests in the year 2015/16, an increase from 2014/15 of 8%. It should be noted that the volume of requests does not give an indication of the amount of time spent in responding to each one. Some requests involve reporting on data that we routinely collect and can be completed relatively quickly, but others 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".

2.26   The main themes of the requests have been identified as:

- IT Contracts;

- CAMHS Services;

- Continuing Healthcare and Personal Health Budgets;

- Commissioning of Services;

- Prescribing Formulary;

- Spend on Agency Staff and GP Locums;

- CCG Contracts and spend.

2.27   Of the applicants the majority have been from:

- IT Contractors;

- General Contractors/Companies;

- Recruitment Agencies;

- Journalists;

- Parliamentary Groups;

- Researchers and Students.

Requests for Internal Reviews

2.28   If an applicant is dissatisfied with the response the CCG has provided they can request an internal review. During 2015/16 one request was received for an internal review.

3.   Conclusion

3.1   Dorset CCG has robust processes for managing IG and the associated responsibilities that come with the commitment to adopt best practice policy and procedures in order to protect patient and service users' information. There is an action plan in place to refresh and improve compliance with the IGT standards.

3.2   We must continue to respond to the challenges faced by changing working practices in order to ensure that we keep pace with the current ever-changing information society. Going forward, this will become more demanding. Developments, such as the introduction of the new General Data Protection Regulations, will have a bearing on the direction of the Information Governance programme.

3.3   The IG Team will continue to deliver an effective service and aim for continuous improvement for 2016/17, and onwards, to ensure that the CCG meet the needs of all services.

3.4   The Governing Body is asked to receive and note this report.

Authors' Names and Titles:	Joyce Green, Head of Information Governance/Customer Care
Telephone Number:	01305 361252

9.7

APPENDICES	
Appendix 1	**IG Toolkit Key Requirements**
Appendix 2	**IG Toolkit Assessment Summary Report 2015/16**

IG Toolkit Key Requirements

Req No	Description
Information Governance Management	
130	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda
131	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans
132	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations
133	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation
134	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained
Confidentiality and Data Protection Assurance	
230	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs
231	Staff are provided with clear guidance on keeping personal information secure, on respecting the confidentiality of service users, and on the duty to share information for care purposes
232	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
234	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data
235	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
236	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines
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
250	Individuals are informed about the proposed uses of their personal information
Information Security Assurance	
340	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs
341	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed
342	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority
343	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use
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
345	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy
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
347	Policy and procedures are in place to ensure that Information Communication Technology (ICT)

	networks operate securely
348	Policy and procedures ensure that mobile computing and teleworking are secure
349	There are documented incident management and reporting procedures
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
351	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures
352	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate
Clinical Information Assurance	
420	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience
421	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements

Information Governance Management

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Total Req'ts	Overall Score	Self-assessed Grade ⑦	Reviewed Grade ⑦	Reason for Change of Grade ⑦
Version 13 (2015-2016)	Published	0	0	3	2	5	80%	Satisfactory	Satisfactory	n/a

Confidentiality and Data Protection Assurance

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Total Req'ts	Overall Score	Self-assessed Grade ⑦	Reviewed Grade ⑦	Reason for Change of Grade ⑦
Version 13 (2015-2016)	Published	0	0	6	2	8	75%	Satisfactory	Satisfactory	n/a

Information Security Assurance

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Total Req'ts	Overall Score	Self-assessed Grade ⑦	Reviewed Grade ⑦	Reason for Change of Grade ⑦
Version 13 (2015-2016)	Published	0	0	13	0	13	66%	Satisfactory	Satisfactory	n/a

Clinical Information Assurance

Assessment	Stage	Level 0	Level 1	Level 2	Level 3	Total Req'ts	Overall Score	Self-assessed Grade ⑦	Reviewed Grade ⑦	Reason for Change of Grade ⑦
Version 13 (2015-2016)	Published	0	0	2	0	2	66%	Satisfactory	Satisfactory	n/a

			Overall						
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade** ⑦	**Reviewed Grade** ⑦	**Reason for Change of Grade** ⑦
Version 13 (2015-2016)	Published	0	0	24	4	28	71%	Satisfactory	Satisfactory	n/a