9.6

NHS DORSET CLINICAL COMMISSIONING GROUP

GOVERNING BODY

ANNUAL REVIEW OF THE INFORMATION GOVERNANCE TOOLKIT

Date of the meeting	19/07/2017
Author	J Green, Head of Information Governance/Customer Care
Sponsoring Clinician	Dr S Yule, Locality Chair for North 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 NHS Digital (formerly known as the Health and Social Care Information Centre) 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 serious IG incidents and to provide an update on 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.

2. Information Governance

Information Governance Internal Accountability/Responsibility

2.1 The Information Governance Group (IGG) met on a bi-monthly basis during 2016/17. 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 2016/17, in relation to the IGT and amendments to the 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 2016/17

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 was required to be submitted no later than 31 March 2017. 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 14 of the 2016/17 IGT and the score as 72%, satisfactory.

2.8 The submission for 2016/17 took place in March 2017. The CCG achieved an overall score of 'Satisfactory' with 23 criteria at level 2 and 5 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 7 requirements and attended an IG Training session. A substantial assurance opinion was issued as follows:

- the CCG had provided sufficient evidence to support its self-assessed scores and no recommendations are required;
- the CCG's in-house IG training materials were reviewed and found to be fully comprehensive;
- a deep dive into the CCG's monitoring and auditing of staff access to confidential information provided satisfactory assurance with respect to this process.

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 14-134 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 2016/17 Dorset CCG achieved 100% of staff attending. This has been verified by the Workforce Team.

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

2.13 Dates for mandatory IG Training for 2017/18 have been issued. Training material is being revised to ensure currency.

Policies and Procedures

2.14 The IG and associated policies have been updated. These are available to staff on the CCG Intranet and to the public on the Dorset CCG Website.

Privacy Notice (Fair Processing)

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

Data Breaches

2.16 The CCG had no serious untoward incidents in relation to IG for 2016/17 and has not been subject to any Information Commissioner Data protection monetary penalties.

2.17 In line with the recommendations of Dame Fiona Caldicott's Information Governance Review, 2013, all activities that involve the use, or sharing, of confidential personal information that do not have a lawful basis must be reported as an IG Serious Incidents Requiring Investigation (SIRI). This is also a requirement of the IGT and has to be evidenced.

2.18 The IG Team have completed a Data Mapping exercise, identifying confidential personal data used/held/shared by the CCG.

2.19 The legal basis for all flows of personal information as in 2.19 have been identified and documented.

2.20 There are none that require reporting as an IG SIRI.

2.21 During the exercise it was identified that a number of IG procedures were not being implemented correctly, especially in the area of manual encryption of emails. This is being addressed via IG Training sessions and monitoring.

2017/18 Improvement Plan

2.22 The IG Team within the CCG is dedicated toward continual improvement in accordance with the IGT/National legislation. It is acknowledged that new Data Protection legislation (detailed below) which includes stronger information rights, will bring challenges.

New General Data Protection Legislation

2.23 The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018 and is currently being phased in as new guidance is made available. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2.24 The primary objectives of the GDPR are to give individuals control of their personal data and to simplify the regulations for international organisations by unifying the regulation within the EU.

2.25 It is expected that the new IGT will also reflect the requirements of the replacement law for the Data Protection Act.

2.26 The IG Team have begun the work required to meet the requirements of both the recommendations and the GDPR.

Freedom of Information

2.27 The CCG received 336 FOI requests in the year 2016/17, an increase from 2015/16 of 5%. 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".

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

- IT Contracts;
- Spend on Consultancy/Agencies;
- Continuing Healthcare and Personal Health Budgets;
- Closure of GP Practices;
- Sustainability and Transformation Plan;
- Commissioning of Services;

- Private Health Providers;
- Prescribing Formulary;
- Spend on Consultant Firms/Agency Staff and GP Locums;
- CCG Contracts and spend.

2.29 Of the applicants the majority have been from:

- IT Contractors;
- General Contractors/Companies;
- Recruitment Agencies;
- Journalists;
- Parliamentary Groups;
- Members of the Public;
- Researchers and Students.

Requests for Internal Reviews

2.30 If an applicant is dissatisfied with the response the CCG has provided they can request an internal review. During 2016/17 no requests were 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 2017/18, 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

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

Clinical Commissioning Group Version 14 (2016-2017)

Requirements List

Req No	Description
Information Governance Management	
14-130	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda
14-131	There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans
14-132	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations
14-133	Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation
14-134	Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained
Confidentiality and Data Protection Assurance	
14-230	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs
14-231	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
14-232	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
14-234	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data
14-235	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
14-236	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines
14-237	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
14-250	Individuals are informed about the proposed uses of their personal information
Information Security Assurance	
14-340	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs
14-341	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed
14-342	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority
14-343	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use
14-344	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
14-345	An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy

14-346	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
14-347	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely
14-348	Policy and procedures ensure that mobile computing and teleworking are secure
14-349	There are documented incident management and reporting procedures
14-350	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
14-351	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures
14-352	The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate
Clinical Information Assurance	
14-420	The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience
14-421	There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements

Report Results

Organisations which this Assessment covers
NHS Dorset CCG

Information Governance Management										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14 (2016-2017)	Published	0	0	3	2	5	80%	Satisfactory	n/a	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**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14 (2016-2017)	Published	0	0	6	2	8	75%	Satisfactory	n/a	n/a

Information Security Assurance										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14 (2016-2017)	Published	0	0	12	1	13	69%	Satisfactory	n/a	n/a

Clinical Information Assurance										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14 (2016-2017)	Published	0	0	2	0	2	66%	Satisfactory	n/a	n/a

9.6

Overall										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed Grade**	**Reviewed Grade**	**Reason for Change of Grade**
Version 14 (2016-2017)	Published	0	0	23	5	28	72%	Satisfactory	n/a	n/a

Grade Key

Not Satisfactory	Not evidenced Attainment Level 2 or above on all requirements (Version 8 or after)
Satisfactory with Improvement Plan	Not evidenced Attainment Level 2 or above on all requirements but improvement actions provided (Version 8 or after)
Satisfactory	Evidenced Attainment Level 2 or above on all requirements (Version 8 or after)