9.7

NHS DORSET CLINICAL COMMISSIONING GROUP

GOVERNING BODY

INFORMATION GOVERNANCE TOOLKIT REPORT

Date of the meeting	15/07/2015
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 NHS Information Governance (IG) is a framework for handling personal information about patients and employees in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It provides consistent standards enabling employees to deal with the many different information handling requirements.

1.2 Effective information governance 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 Information Governance Toolkit (IGT) draws together the legal rules and central guidance set out by Department of Health policy and presents them in a single standard as a set of IG requirements.

1.4 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.

1.5 The IGT performance results provide assurance and are monitored by the HSCIC and used by the Care Quality Commission, the Audit Commission and shared with the Information Commissioner's Office. The results are also freely available to the public and are required to be published in the CCG's Annual Report.

1.6 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 2014/15. This group is chaired by the Senior Information Risk Officer (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 2014/15, in relation to the IGT and the development and approval of core IG framework policies and procedures.

2.3 The CCG has established an approach to IG that ensures the organisation (from Governing Body level down) has the ability to fully comply with its requirements in terms of data protection and confidentiality.

2.4 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 2014/15

2.5 The IGT is produced by the Department of Health via the Health and Social Care Information Centre (HSCIC). It draws together the relevant information management legislation, national and international guidance under a single framework.

2.6 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.

2.7 The CCG is required to measure itself against 28 requirements. These are broken down into the levels in fig 1 below. Each level contains several questions all of which require supporting evidence to be submitted. In total this requires several hundred individual items of evidence.

NR	Not relevant
0	No or insufficient evidence, not satisfactory for compliance
1	Limited evidence, not satisfactory for compliance
2	Minimum level satisfactory for compliance
3	Evidence of further processes, measures & controls, satisfactory for compliance

Fig 1.

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

2.9 The IGG verified the submission of version 12 of the 2014/15 IGT and the score as 70%, satisfactory.

2.10 The submission for 2014/15 took place on 31st March 2014. The CCG achieved an overall score of 'Satisfactory' with 25 criteria at level 2 and 3 criteria at level 3. See appendix 1.

2.11 Prior to submitting its final assessment, the CCG's internal auditors, TIAA audited a sample of 10 requirements and attended an IG Training session. Their overall opinion was '*Information Governance requirements and scoring criteria represent a high-level self-assessment of performance within the CCG*'.

2.12 The Governing Body can take assurance that the controls upon which the organisation relies to manage IG are consistently applied and effective. See Appendix 2 Internal Audit Report.

Information Governance Training

2.13 In order to comply with requirement 12-134 of the IG Toolkit staff attendance at the training is mandatory and has to be repeated annually. To allow for long term sickness, maternity leave etc., 95% of staff attending is acceptable. In 2014/15 Dorset CCG achieved the following 99.7% of staff attending. This has been verified by Workforce.

2.14 Dates for mandatory IG Training for 2015/16 are currently being determined. Training material to be revised to ensure currency.

Caldicott2 IG review recommendations

2.15 The above recommendations are still being implemented nationally and will form the basis of version 13 of the IGT.

COMPLIANCE WITH LEGAL AND REGULATORY FRAMEWORK

2.16 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

2.17 The CCG received 293 FOI requests in the year 2014/15, almost exactly the same as last year (279). 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".

2.18 There have been no complaints made by requesters to date. The CCG is increasingly receiving requests from staff at other NHS Trusts and organisations using the Act as a quicker way of attaining information. FOIA remains a challenge to manage and for different areas of the CCG to respond to.

2.19 In order to meet the requirements of best practice as detailed in the ICO's model publication scheme the CCG publishes anonymised completed requests on the public facing website in the form of a disclosure log. The disclosure log also builds a knowledge library of information which external applicants can access so hopefully reducing the number of requests received by the CCG.

Serious Untoward Incidents

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

Information Commissioner Notices

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

New powers given to the ICO

2.22 From 1 February 2015, the ICO can subject public healthcare organisations to a compulsory audit under section 41A of the Data Protection Act. These have previously only applied to central government departments.

2.23 The audits review how the NHS handles patients' personal information, and can review areas including security of data, records management, staff training and data sharing.

2.24 To date, the ICO has issued fines totalling £1.3m to NHS organisations.

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. National developments 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 2015/16, 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 Assessment Summary Report 2014/15**
Appendix 2	**IGT Audit Report**

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 12 (2014-2015)	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 12 (2014-2015)	Published	0	0	7	1	8	70%	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 12 (2014-2015)	Published	0	0	13	0	13	66%	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 12 (2014-2015)	Published	0	0	2	0	2	66%	Satisfactory	n/a	n/a

Overall										
Assessment	**Stage**	**Level 0**	**Level 1**	**Level 2**	**Level 3**	**Total Req'ts**	**Overall Score**	**Self-assessed**	**Reviewed Grade**	**Reason for Change of Grade**

9.7

								Grade		
Version 12 (2014-2015)	Published	0	0	25	3	28	70%	Satisfactory	n/a	n/a

tiaa

INTERNAL AUDIT

NHS Dorset Clinical Commissioning Group

Information Governance Toolkit v12

2014/15

DRAFT

9.7

March 2015

Executive Summary

OVERALL ASSURANCE ASSESSMENT

KEY FINDINGS

- **The CCG had provided sufficient evidence to support its self-assessed scores and no recommendations are required.**

SCOPE

The objective of the audit was to assess the adequacy of policies, systems and operational activities to complete, approve and submit the IGT scores. An opinion on the validity of the scores within the sample is based on the evidence available at the time of the audit.

ACTION POINTS

Urgent	Important	Routine	Operational
0	0	0	0

Management Action Plan - Priority 1, 2 and 3 Recommendations

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
No recommendations.							

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.
2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.
3	ROUTINE	Control issue on which action should be taken.

Operational Effectiveness Matters

Ref	Risk Area	Item	Management Comments
No Operational Effectiveness Matters were identified.			

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures, rather than on a one-by-one basis

Detailed Findings

INTRODUCTION

1. This review was carried out in February 2015 as part of the planned internal audit work for 2014/15. Based on the work carried out an assessment of the adequacy of the arrangements to mitigate the key control risk areas is provided in the Executive Summary.

2. Over the past few years, NHS organisation compliance with the requirements of the NHS Information Governance Toolkit (IGT) has steadily increased, and since 2010/11 all NHS organisations have been required to demonstrate compliance with at least level 2 attainment against all IGT requirements, and to be independently audited. This level of required compliance continues to apply during 2014/15.

KEY FINDINGS & ACTION POINTS

3. The key control and operational practice findings that need to be addressed in order to strengthen the control environment are set out in the Management and Operational Effectiveness Action Plans. Recommendations for improvements should be assessed for their full impact before they are implemented.

4. Appendix A provides a summary of the requirements reviewed showing the CCG score alongside the score validated by available evidence. Appendix B provides further details on the findings of the assessment of each of the requirements tested.

SCOPE AND LIMITATIONS OF THE REVIEW

5. The aim of the review was to evaluate the extent to which the CCG had established controls to manage the following risks:

- The CCG may fail to meet adequate levels of compliance and / or may be taking inadequate action to improve areas of weakness. Therefore exposing itself to possibly serious consequences because of unauthorised access to, or loss, damage or destruction of confidential, personal and sensitive information in its care. Consequently the organisation may be exposed to financial penalties or reputational damage.
- The assessment process may be flawed so that the return may be invalid, providing the CCG with false assurance on the security and governance of its information.

6. In writing this report the following key areas were considered:

- The internal governance process
- Validity of returns
- Wider risk exposures
- National IG Initiatives

7. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan. The testing was limited to the following sample of 10 of (28 IGT) requirements which was agreed with management:

- 130, 132, 230, 231, 234, 340, 341, 342, 343, and 348

MATERIALITY

8. The Information Commissioner's Office has the power to issue monetary penalty notices of up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010, and serious breaches of the Privacy and Electronic Communications Regulations.

DISCLAIMER

9. The matters raised in this report are only those that came to the attention of the auditor during the course of the internal audit review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

10. Information Governance requirements and scoring criteria represent a high-level self-assessment of performance within the CCG. Audit review and opinion is based upon the evidence available to substantiate the score submitted in relation to these high level requirements and criteria, at the time of the audit. Audit opinions are based upon the reasonableness of the scores in these circumstances and do not, therefore, infer assurance that detailed controls are adequate to meet business needs. It is possible, therefore, that more detailed audits of specific areas contained within the IG Toolkit may uncover control weaknesses which subsequently appear to contradict the opinions provided by this report.

RISK AREA ASSURANCE ASSESSMENTS

11. The definitions of the assurance assessments are:

Substantial Assurance	Based upon our findings there is a robust series of suitably designed internal controls in place upon which the organisation relies to manage the risk of failure of the continuous and effective achievement of the objectives of the process, which at the time of our review were being consistently applied.
Reasonable Assurance	Based upon our findings there is a series of controls in place, however there are potential risks that they may not be sufficient to ensure that the individual objectives of the process are achieved in a continuous and effective manner. Improvements are required to enhance the adequacy and effectiveness of the controls to mitigate these risks.
Limited Assurance	Based upon our findings the controls in place are not sufficient to ensure that the organisation can rely upon them to manage the risks to the continuous and effective achievement of the objectives of the process. Significant improvements are required to improve the adequacy and effectiveness of the controls.
No Assurance	Based upon our findings there is a fundamental breakdown or absence of core internal controls such that the organisation cannot rely upon them to manage the risks to the continuous and effective achievement the objectives of the process. Immediate action is required to improve the adequacy and effectiveness of controls.

ACKNOWLEDGEMENT

12. We would like to thank staff for their co-operation and assistance during the course of our work.

RELEASE OF REPORT

13. The table (Figure 1) below sets out the history of this report.

Figure 1 - Report History

Date draft report issued:	3rd March 2015
Date management responses recd:	
Date final report issued:	

14. The following matters were identified in reviewing the Key Risk Control Objective:

Governance: Failure to direct the process through approved policies, procedures, structures and processes may lead to information breaches.

14.1 The CCG's Information Governance Policy, Framework & Strategy (reviewed on 26th November 2014) sets out the process, governance arrangements and policy framework for the delivery of safe and effective information governance within the CCG and for any services commissioned by the CCG. The CCG's Information Governance Group reports to the Audit and Quality Committee which in turn reports to the Governing Body.

14.2 Evidence to demonstrate compliance with the toolkit requirements had been uploaded to the HSCIC's online IG Toolkit. Evidence containing personal and/or confidential information had been stored in a local evidence folder on the CCG's network.

14.3 The CCG took the decision to reset the scoring of all 28 IGT requirements to level zero in order to rescore each requirement as and when evidence became available for uploading to the IGT to ensure accurate scoring. This is considered best practice, but is not usually implemented within organisations as a result of the evidence 'roll over' functionality on the IGT. Audit therefore considered the process at the CCG to be exemplar.

Validity of Returns: Failure to comply with the requirements of the Information Governance Toolkit could invalidate the self-assessment.

14.4 Audit have agreed with the current scoring of 10 of 10 requirements reviewed. The details of TIAA's conclusions have been included in Appendix B, but are summarised below:

- 8 Level 2 scores were agreed.
- 2 Level 3 scores were agreed.

Wider Risk Exposure: Non-compliance with requirements may lead to information breaches, fines from the Information Commissioner and damage to the CCG's reputation.

14.5 At the time of the review there had not been any externally reportable IG Incidents and the CCG was not anticipating any issues in meeting the requirement for 95% of staff to complete their annual IG training. Approximately 99% of staff had completed their IG training, with the remainder scheduled to do their training in February and March.

14.6 The CCG uses facilitated departmental IG training sessions to deliver mandatory IG training rather than using the NHS IG online Training Tool. As part of Requirement 12-134 (Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained) locally delivered training materials and plans must be checked for equivalence to materials in the NHS IG Training Tool, by auditors.

14.7 Audit attended one of the departmental IG training sessions.

In summary, the training covered:

- Overview of information governance including roles and responsibilities within the CCG.
- The Data Protection Act and each of the 8 Principles.
- Records Management
- The Caldicott Principles
- NHS Constitution
- Freedom of Information
- Information Security
- Relevance of IG to contracts.

14.8 The training was very interactive and included regular group quizzes. It was noted that the staff who attended took the IG training seriously and were fully engaged with the presentation and subject matter.

14.9 IG training was discussed with the Information Governance and Customer Care Manager.

14.10 Satisfactory assurance was obtained that the local information governance training materials developed by the Information Governance Team are equivalent to the materials held in the NHS IG Training Tool.

14.11 Audit performed a detailed walk-through of the IG Toolkit with the IG Manager for the 10 requirements within the sample to identify where further actions were required and to provide advice/guidance on the requirements. A number of additional actions were consequently identified and added to the action list during the course of the review.

14.12 Overall the CCG was reporting Level 1 for 2 of the IGT requirements, 22 at Level 2 and 3 at Level 3 with 1 not yet answered. Action plans were in place to refresh evidence through to 31st March 2015 to strengthen and/or increase the current scores. The review of toolkit scores and the IG incident reporting process did not indicate any areas of wider risk exposure,

National IG Initiatives: Pseudonymisation

14.13 Requirement 12-352 'The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate' has been self-assessed at a Level 2 by the CCG.

14.14 It was noted that the CCG has Sophos SafeGuard Port Control software installed on its network to help prevent data loss.

Appendix A

IGT Position Status

The following table summarises the requirements that fall within the sample and is designed to show how the score claimed by the CCG compares to the level supported by currently available evidence. Also indicated is the probable score should all of the actions listed in the IGT action plan be completed satisfactorily.

Requirement Number	CCG Score	Available Evidence Score	Possible Year-End Score from Action Plan
130	L3	L3	L3
132	L2	L2	L2
230	L3	L3	L3
231	L2	L2	L2
234	L2	L2	L2
340	L2	L2	L2
341	L2	L2	L2
342	L2	L2	L2
343	L2	L2	L2
348	L2	L2	L2

Appendix B

IGT Requirements Analysis

No	Requirement	Level Claimed	Auditor Conclusion	Auditor Explanation	Assessment	Recommendations
12-130	There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda.	L3	L3 - The CCG successfully met Level 3 compliance.	The CCG has provided sufficient evidence that there is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda.	Agree	None.
12-132	Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations.	L2	L2 - The CCG successfully met Level 2 compliance.	The CCG has provided sufficient evidence to demonstrate that formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations.	Agree	None.
12-230	The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs.	L3	L3 - The CCG successfully met Level 3 compliance.	The CCG has provided sufficient evidence that the Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs.	Agree	None.

No	Requirement	Level Claimed	Auditor Conclusion	Auditor Explanation	Assessment	Recommendations
12-231	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.	L2	L2 - The CCG successfully met Level 2 compliance.	The CCG has provided sufficient evidence that 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.	Agree	None.
12-234	There are appropriate procedures for recognising and responding to individuals' requests for access to their personal data.	L2	L2 - The CCG successfully met Level 2 compliance.	The CCG has provided sufficient evidence to demonstrate that there are appropriate procedures for recognising and responding to individuals' requests for access to their personal data.	Agree	None.
12-340	The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs.	L2	L2 - The CCG successfully met Level 2 compliance.	The CCG has provided sufficient evidence to demonstrate that the Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs.	Agree	None.
12-341	A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed.	L2	L2 - The CCG successfully met Level 2 compliance.	The CCG has provided sufficient evidence that a formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed.	Agree	None.

No	Requirement	Level Claimed	Auditor Conclusion	Auditor Explanation	Assessment	Recommendations
12-342	There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority.	L2	L2 - The CCG successfully met Level 2 compliance.	The CCG has provided sufficient evidence to demonstrate that there are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority.	Agree	None.
12-343	Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use.	L2	L2 - The CCG successfully met Level 2 compliance.	The CCG has provided sufficient evidence to demonstrate that monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use.	Agree	None.
12-348	Policy and procedures ensure that mobile computing and teleworking are secure.	L2	L2 - The CCG successfully met Level 2 compliance.	The CCG has provided sufficient evidence to demonstrate that policy and procedures ensure that mobile computing and teleworking are secure.	Agree	None.