9.5

NHS DORSET CLINICAL COMMISSIONING GROUP

GOVERNING BODY MEETING

ANNUAL REVIEW OF THE INFORMATION GOVERNANCE TOOLKIT

Date of the meeting	18/07/2018
Author	J Green, Head of Information Governance
Sponsoring Board member	S Hunter, Chief Finance Officer
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	Patients/members of the public are involved in the management of complaints.
Previous GB / Committee/s, Dates	Audit and Quality Committee; 04 July 2018

Monitoring and Assurance Summary

This report links to the following Strategic Objectives	• Integrated Community and Primary Care Services • One Acute Network • Digitally Enabled Dorset • Leading and Working Differently

	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	✓		✓
Freedom of Information	✓		✓
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 has had to demonstrate compliance with Information Governance (IG) requirements by completing the Information Governance Toolkit (IGT).

1.2 There has been a requirement for all NHS organisations to meet the minimum of level 2 across all requirements within the IGT. However, year on year, the CCG has sought 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.

1.3 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.

1.4 From April 2018, the Data Security and Protection (DSP) Toolkit replaces the Information Governance (IG) Toolkit as the standard for cyber and data security for healthcare organisations.

1.5 As well as the implementation of the DSP Toolkit the General Data Protection Regulations (GDPR) came into force on the 25th May 2018 as did the new Data Protection Bill (DPA 2018).

2. Information Governance

Information Governance Internal Accountability/Responsibility

2.1 The Information Governance Group (IGG) met on a bi-monthly basis during 2017/18. The group is chaired by the Head of IG/Data Protection Officer and is attended by the Caldicott Guardian, 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 2017/18, 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 2017/18

2.4 The IGT for 2017/18 was a similar version to the previous year and entitled version 14.1. NHS Digital did not change the requirements as they were planning for the new Data Security and Protection Toolkit which was to be introduced for 2017/18/

2.5 The toolkit required 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. A full assessment was required to be submitted no later than 31 March 2018. This required uploading the evidence of compliance against the key factors in order to obtain a score.

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

2.8 The IGG verified the submission of version 14.1 of the 2017/18 IGT and the score as 75%, satisfactory.

2.9 The submission for 2017/18 took place in March 2018. The CCG achieved an overall score of ‘Satisfactory’ with 21 criteria at level 2 and 7 criteria at level 3. (See appendix 2).

Audit Findings

2.10 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;

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

Data Breaches

2.12 The CCG had no serious untoward incidents in relation to IG for 2017/18 and has not been subject to any Information Commissioner Data Protection monetary penalties.

Data Security and Protection (DSP) Toolkit

2.13 NHS Digital has now closed the IG Toolkit and replaced it with the DSP Toolkit. This is based on the National Data Guardian’s Review of Data Security, Consent and Opt-Outs which sets out ten data security standards (see appendix 1).

2.14 The IG Toolkit assessed performance against four levels 0, 1, 2 and 3. Organisations were required to provide evidence of compliance with (at least) level 2 for all elements of their assessment. The DSP Toolkit does not include levels and instead requires compliance with “assertions” and (mandatory) evidence items.

2.15 Examples of assertions from the DSP Toolkit are:

- There are clear data security and protection policies in place and these are understood by staff and available to the public;

- Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4);

- Personal information processed by the organisation is adequate (and not excessive) for the purposes;

- Leaders and board members receive suitable data protection and security training;

- Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration.

Data Security and Protection Group

2.16 The current IG Group will now be renamed the Data Security Protection Group to be in line with the Data Security and Protection Toolkit.

General Data Protection Regulations (GDPR)

2.17 The GDPR became law on 25th May 2018.The Information Governance Alliance has produced an excellent guidance document highlighting what is new in the law and what is similar. In particular, they have produced a list of “Headline Impacts” which are:

- The new accountability requirement means organisations are now required, not only to comply with the new law, but to demonstrate that they comply with the new law;

- keep records of data processing activities;

- there is a legal requirement for personal data breach notification to the ICO within 72 hours where there is a risk to data subjects;

- removal of charges, in most cases, for providing copies of records to patients or staff who make a subject access request;

- appointment of Data Protection Officer - mandatory for all public authorities;

- Data Protection Impact Assessment, formerly called a Privacy Impact Assessment, required for high risk processing;

- Data Protection issues must be addressed in all information processes at an early stage;

- Specific requirements for transparency and the provision of information to data subjects about how their information is used;

- Tighter rules on consent where this is used as a basis for lawful processing.

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

2.18 It has to be noted that guidance is still being released in relation to the GDPR and as yet not all is available.

2.19 The new law takes the Data Protection Act 1998 and strengthens it. As the CCG already meets the requirements of the DPA 1998 we are well placed to meet the requirements of the GDPR with a number of amendments and updates required.

Impact of the GDPR

2.20 At a recent meeting, in June, of the Pan Dorset Information Governance Group the implementation of the GDPR was discussed. It was noted that all the Health and Social Care organisations in Dorset were at the same point.

2.21 It was agreed by all that no organisation will ever be fully compliant with the GDPR as it is a continual work in progress as was compliance with the Data Protection Act 1998.

Data Protection Bill

2.22 The Data Protection Bill was announced in the Queen's Speech on 21 June 2017. The aim of the Bill is to modernise the data protection laws in the UK to make them fit-for purpose for the expanding digital economy and society.

2.23 As part of the Bill the EU's GDPR standards will be applied. The government aims to ensure that modern, innovative uses of data can continue while at the same time strengthening the control and protection individuals have over their data.

2.24 The Bill includes a number of agreed modifications to the GDPR to make it work for the benefit of the UK in areas such as academic research, financial services and child protection. Together the GDPR and the Data Protection Bill form the Data Protection Act 2018.

2.25 The main elements of the Bill are:

General Data Processing

- Implement GDPR standards across all general data processing;

- Provide clarity on the definitions used in the GDPR for the UK;

- Ensure that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health and safeguarding situations can be maintained;

- Provide appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes;

- Set the age from which parental consent is not needed to process data online at age 13, supported by a new age-appropriate design code enforced by the Information Commissioner.

2018/19 Improvement Plan

2.26 The IG Team within the CCG is dedicated toward continual improvement in accordance with the Data Protection Act (DPA) 2018.

2.27 Work on ensuring the CCG meets the requirements of the DPA 2018 continues. Presently the IG Team are working on:

- updating policies and documentation that the CCG has in use;

- renewing the CCGs Privacy Notice;

- updating staff and public information booklets;

- reviewing the PIA procedure;

- linking information flows to the legal basis for processing.

2.28 The GDPR action plan, which is regularly reviewed by the IG Group, is still being worked to and good progress is being made.

Freedom of Information

2.29 The CCG received 315 FOI requests in the year 2017/18, a decrease from 2016/17 of 6%. 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”.

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

- Continuing Healthcare and Personal Health Budgets;

- Sustainability and Transformation Plan;

- Commissioning of Services, especially Mental Health;

- Individual patient Treatments, especially IVF;

- Prescribing Formulary;
- Primary Care;
- IT Contracts and spend.

Requests for Internal Reviews

2.31 If an applicant is dissatisfied with the response the CCG has provided they can request an internal review. During 2017/18 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 The CCG has achieved a satisfactory submission for the IGT for 2017/18, however, the IG Team, with the assistance of representatives from the DSP Group, need to continue to ensure that the CCG complies with the requirements of the new Data Protection Act 2018 (which includes the details of the GDPR) and the DSP Toolkit.

3.3 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 363567

9.5

APPENDICES	
Appendix 1	**10 Data Security Standards**
Appendix 2	**IG Toolkit Assessment Summary Report 2017/18**

Appendix 1

The National Data Guardian's Review of Data Security, Consent and Opt-Outs has set out ten data security standards. These are listed below:

Data Security Standard 1

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

Data Security Standard 2

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3

All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Data Security Standard 4

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5

Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6

Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Data Security Standard 8

No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian’s Data Security Standards.

9.5

Version 14.1 IGT Report **Appendix 2**

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 14.1 (2017-2018)	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 14.1 (2017-2018)	Published	0	0	5	3	8	79%	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 14.1 (2017-2018)	Published	0	0	11	2	13	71%	Satisfactory	n/a	n/a

9.5

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 14.1 (2017-2018)	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 Grade ?	Reviewed Grade ?	Reason for Change of Grade ?
Version 14.1 (2017-2018)	Published	0	0	21	7	28	75%	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)