NHS
Northumberland
Clinical Commissioning Group

Information Governance Annual Report

Northumberland CCG

2018/19

Contents

1. Introduction 2
2. 2018/19 DSPT Performance 2
2.1 Self-Assessment Results 2
2.2 Audit 3
3. Strategy 4
4. DSP Toolkit 2019/20 4
5. Training 4
6. Policy Review 5
7. Freedom of Information and Subject Access Requests 5
8. Key Performance Indicators 6
9. Risks 7
10. Incidents 7
11. Reporting 8
12. IG compliance assurance within the Commissioning Support Unit 8
13. Summary 8

1. Introduction

Information Governance is the framework that brings together a number of information related requirements.

These legal requirements were developed to ensure confidentiality/protection of information in all formats, electronic and paper and to support appropriate information sharing for patient care.

The Data Security & Protection Toolkit (DSPT), which was introduced in 2018 and replaced the former Information Governance Toolkit, has been provided by NHS Digital to support performance monitoring of progress on Information Governance in the NHS. NHS Digital uses the toolkits to monitor performance and as evidence that organisations are compliant with the IG SoC (Information Governance Statement of Compliance).

The DSPT is made up of 10 sections, which equate to the 10 National Data Guardian Standards. Although the CCG, as a public authority and statutory body, is subject to the provisions of the Freedom of Information Act, NHS Digital has not included Corporate Information Assurance in the DSPT. However this report includes CCG performance against its statutory duty to comply with the Freedom of Information Act 2000.

This report covers the CCG's performance against its Information Governance responsibilities during the year.

2. 2018/19 DSPT Performance

2.1 Self-Assessment Results

Throughout 2018/19 progress was made in the DSPT to develop processes and ensure that information governance principles and understanding continued to be embedded throughout the organisation. Regular meetings with the Corporate Affairs Manager demonstrated steady progress with this, together with the collation of evidence and population of the DSPT ready for the final submission in March 2019.

Each component of the DSPT has a number of assertions to meet the standard. These are as follows:

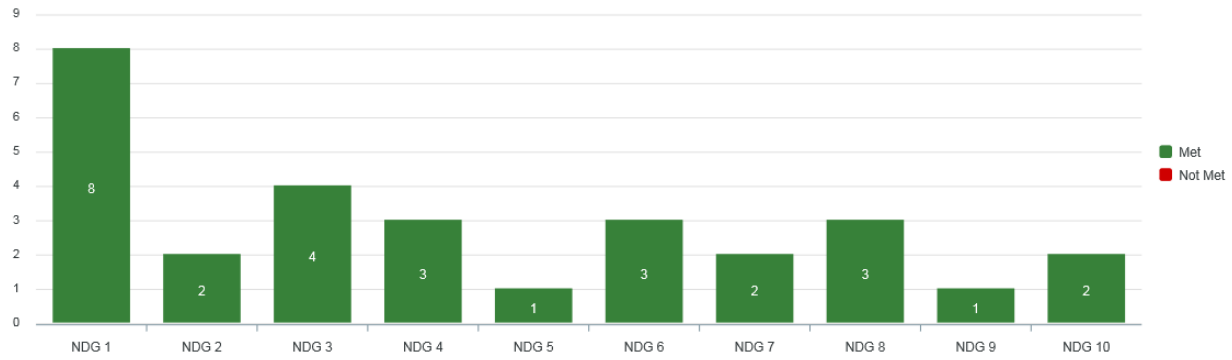
Standard	**Definition**
NDG 1	Personal confidential data
NDG 2	Staff responsibilities
NDG 3	Training
NDG 4	Managing Data Access

NDG 5	Process Reviews
NDG 6	Responding to Incidents
NDG 7	Continuity Planning
NDG 8	Unsupported Systems
NDG 9	IT Protection
NDG 10	Accountable Suppliers

Each of the assertions contains a number of sub-assertions which must be answered if mandatory. Non-mandatory assertions are optional. In the 2018/19 DSPT 70 assertions were mandatory.

The CCG self-assessed against the DSPT for 2018/19 and met all of the mandatory assertions, therefore achieving a 'Standards Met' assessment. It is no longer a function of the DSPT to offer the option to apply for exemptions; therefore all the mandatory assertions were answered.

The figure below shows the 10 National Data Guardian Standards and their status.



2.2 Audit

A sample of 18 assertions of the CCG's DSPT was audited by AuditOne. There were no recommendations to report from the audit (see table below), however due to the timing of the audit running parallel to the collation of evidence, there was recognition that some items of evidence were not available on the initial review by Audit, but were subsequently provided. The CCG and North of England Commissioning Support Unit (NECS) continued to work to ensure that evidence was populated at the earliest possible stage throughout the year.

18/19 Report extract

	Priority		
	High	Medium	Low
Compliance with control framework	0	0	0
Total	**0**	**0**	**0**

3. Strategy

The Information Governance Strategy has been reviewed following the release of the DSPT with changes within the DSPT built into the strategy. The organisation will continue to develop its Information Governance strategy and will be supported by NECS with collecting and populating evidence and with the DSPT action plan. In approving the Strategy, the CCG have also asked that further work be undertaken to ensure that external influences relating to STP and data sharing is more fully taken account of in future iterations. The Strategy also included changes as a result of the General Data Protection Regulation.

An action plan to address the key requirement of GDPR was supplied to the CCG via the IG service and was regularly monitored and updated to ensure all actions were completed.

4. DSP Toolkit 2019/20

At the time of writing this report the new version of the DSPT had not been released. The NECS IG Team will continue to identify changes and inform the CCG of the work required and related evidence for collection in order to meet the DSPT assertions.

The CCG will ensure that any partners they work with meet IG standards and that assurance of this has been given. It is recognised that this is an area that needs further work to provide higher levels of assurance.

The goal will be to comply with all mandatory requirements.

5. Training

The Training Needs Assessment was refreshed for 2018/19. All CCG staff are required to conduct their mandatory training via the NHS Digital online training tool. This was refreshed onto a new platform in 2017 and the basic training was updated and called Data Security Awareness Level1.

The NHS Digital IG Training Tool is an online training tool focused on all aspects of learning. The aim of the tool is to develop and improve staff knowledge and skills in information governance, to support the provision of high-quality health & social care.

To date only the Data Security Awareness module is available. Staff in specialist roles such as the SIRO and Caldicott Guardian can undertake further training and NECS is developing training materials which will be delivered in face to face sessions as required. Compliance reports have been produced by the NECS Organisational Development team throughout the year and presented as part of the Governance Assurance Report at the Governance Group. At the 31st March 2019 the percentage of staff within the CCG having completed IG training was 100%.

6. Policy Review

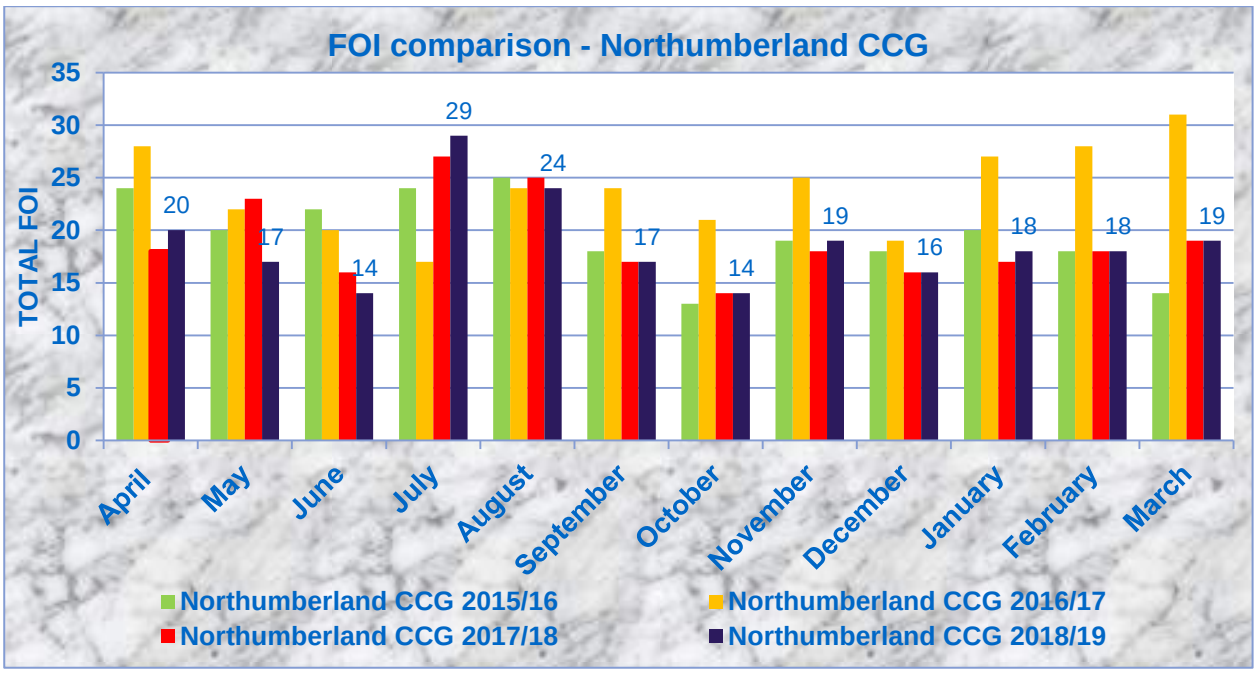
The CCG has, in conjunction with NECS, undertaken a review of IG policies during the report period as agreed by the Joint Locality Executive Board (JLEB). The IG policies will be reviewed on a bi-annual basis for consideration and received approval of the Governance Group and JLEB. Where there is release of new national guidance or legislation, policies are created / amended to reflect this. The IG service within NECS has performed this function for the CCG and will continue to do so in 2019/20. The IG policies were reviewed in May 2018 to include GDPR changes and will be further reviewed in 2020, as follows:

Policy number	Policy Title	Review Date
IG01	Confidentiality and Data Protection Policy	May 2020
IG02	Data Quality Policy	May 2020
IG03	Information Governance & Information Risk Policy	May 2020
IG04	Information Access Policy	May 2020
IG05	Information Security Policy	May 2020
IG06	Records Management Policy & Strategy	May 2020

7. Freedom of Information and Subject Access Requests

Northumberland CCG received 223 Freedom of Information requests in the year 2018/19, compared to 247 in the year 2017/18, 294 in the year 2016/17, 235 in the year 2015/16, 240 in the year 2014/15 and 204 requests received in 2013/14.

All requests were responded to within the statutory 20 working day period. Requests continue to come from a mixture of sources including individuals, organisations, media, MPs and solicitors.



Living individuals (staff or patients/public) can request to see all information that is held about them (known as a Subject Access Requests). There is a legal requirement for the CCG to make this information available upon request and staff have been made aware of this procedure. To support this, a SAR fact sheet has also been produced and circulated to all staff for awareness in staff's knowledge relating to SAR. Advice and guidance will be provided to key staff by the NECS IG team.

SARs are received directly by the CHC team in the Commissioning Support Unit relating to continuing health care funding and other similar requests, therefore, there is ongoing work with the CHC teams and the NECS IG team to receive a monthly report/database identifying the number of SARS that have been received.

There was one Subject Access Request for Northumberland CCG relating to patients or staff received by the NECS corporate Information Governance team in 2018/19. However when clarification was sought the requestor never confirmed therefore the request was withdrawn.

All subject access requests were managed in line with the requirements of the Data Protection Act.

8. Key Performance Indicators

The CCG has two IG KPIs with the NECS:

1. FOI and DPA requests acknowledged within 2 days and responded to within the statutory timescales 100% of the time.
2. Provision of progress report on DSPT.

The NECS IG service processed all FOI and DPA requests within the statutory timescales consistently throughout the year. DSPT progress reports were made available to the CCG and NECS worked with the CCG on a regular basis to enable the CCG to publish at a 'Standards Met' assessment in March 2019.

The DSPT will continue to be monitored via Governance Group. KPIs will continue to be reported by NECS on a regular basis.

The NECS IG team and the CCG Head of Governance will be looking to embed good information governance practice throughout the CCG, checking staff understanding and compliance as well as improving areas identified in the IG work plan and DSPT action plan for 2019/20.

9. Risks

During 2018/19 the CCG reported no information related risks on the risk register. However, reports to the Governance Group demonstrate that risk assessments are being completed on key information assets and there are no major issues arising.

10. Incidents

The CCG has an Incident Reporting and Management Policy in place. This policy is to be used by staff for the recording, reporting and reviewing of information governance (IG) and information security incident/near misses.

During 2018/2019 the CCG had one IG related incident/near miss, which was reported to the Governance Group at the time via the Governance Assurance reports. This related to:

- Incident 57670 reported on 15/01/2019 - NHS Lothian sent an email to the CCG using the Enquiries email address (NORCCG.enquiries@nhs.net), intended for commissioners, which included patient identifiable information.

Incidents of data loss continue to occur across the NHS and in some cases these can be significant and in breach of national guidance. There were no losses of data for Northumberland CCG.

In July 2018, the way in which information governance incidents were to be reported changed. NHS Digital issued the *Guide to the Notification of Data Security and Protection Incidents - Reporting incidents post the adoption of GDPR 25 May 2018 and NIS Directive 10 May 2018*. All NHS organisations are required to assess a potential reportable incident using the guidance and if deemed to be reportable to report via the DSPT. The Information Commissioner's Office (ICO) and Department of Health and will be notified via the DSPT. This new reporting process has been adopted into the CCG's incident reporting policy and procedures.

The CCG has reported no incidents via the DSPT in 2018/2019.

11. Reporting

A quarterly Governance Assurance Report was presented to the Governance Group which has the responsibility for oversight of IG. The quarterly report focuses primarily on:

- Compliance with requests for information
- IG incidents/near misses and data breaches
- DSPT update and current position
- IG training update
- Caldicott Guardian requests and issues

This report has been under review and will change in format for 2019/20 as agreed with the CCG.

12. IG compliance assurance within the Commissioning Support Unit

NECS published a Standards Met DSPT. Progress is monitored regularly for both NECS and CCGs at the NECS IG Committee which takes place every two months. The IG Committee undertakes assurance and scrutiny on behalf of the Executive Group that NECS is managing security and confidentiality of information effectively.

Other regular agenda items at IG Committee include IG Risks, IG Incidents, Security Reports, Systems Reports, Data Protection Impact Assessments, and updates from National Groups, Policies and Procedures and mandatory training.

IG Questionnaire spot checks have been carried out in HR, IFR, Commissioning Finance and Complaints that work across multiple CCGs including Northumberland CCG. Within Northumberland CCG 2018-19 all staff members passed the recommended target score of 32 out of 40.

Confidential compliance walk arounds were conducted in IFR and HR for 2017/18 and all compliance checks audited were passed. The IG team in 2018/19 is still to decide which departments are planned to undergo confidentiality compliance walk arounds. The results of these compliance checks will be conducted on a quarterly basis and reported to the NECS IG Committee and in the Northumberland reports.

13. Summary

The CCG has developed its Information Governance Framework throughout the year. Highlights include;

- Standards Met performance in the DSPT
- 100% compliance with FOI requests
- 100% compliance with SAR requests
- Compliant confidential walk arounds
- 100% CCG staff trained in IG

The CCG has made significant strides in its IG agenda during the year and will continue to build on this.

Author -

Hilary Murphy
Information Governance Officer
North of England Commissioning Support Unit.