Information governance improvement programme and the General Data Protection Regulation

Report to: Board

Date: 17 January 2018

Report by: Rami Okasha, Executive Director of Strategy and Improvement

Report No: B-33-2018

Agenda Item: 17

PURPOSE OF REPORT

To advise members of progress on the Care Inspectorate's information governance improvement programme and preparedness for the General Data Protection Regulation.

RECOMMENDATIONS

That the Board:

1. Notes the report and further work required ahead of May 2018.

Consultation Log

Who	Comment	Response	Changes Made as a Result/Action
Senior Management			
Legal Services			
Corporate and Customer Services Directorate			
Committee Consultation (where appropriate)			
Partnership Forum Consultation (where appropriate)			

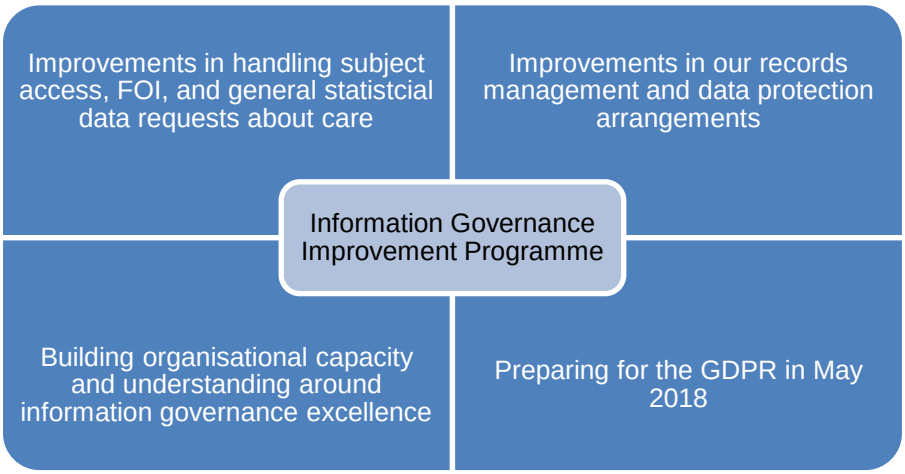
Equality Impact Assessment		
Confirm that Involvement and Equalities Team have been informed	YES ☐	NO X
EIA Carried Out	YES ☐	NO X
If yes, please attach the accompanying EIA and appendix and briefly outline the equality and diversity implications of this policy.		
If no, you are confirming that this report has been classified as an operational report and not a new policy or change to an existing policy (guidance, practice or procedure)	Name: R Okasha Position: Executive Director of Strategy and Improvement	
Authorised by Director	Name: K Reid	Date: 8 January 2018

1.0 BACKGROUND

The Care Inspectorate has a number of data protection obligations, principally around protecting personal data, storing public records effectively, and responding to requests for information. From May 2018, new obligations will exist in the form of the General Data Protection Regulation.

In July 2016, the Executive Team agreed an information governance action plan to accelerate planned improvements to our information governance activities. Part of this involved procuring an information governance consultant to provide external assurance about the quality and progression of the work in the action plan. In November 2016, the consultant was procured to review the work undertaken as part of this action plan and, in February 2017, reported on the Care Inspectorate's information governance activities. The consultants identified the need for significant improvements across a range of areas. The Chief Executive briefed the Resources Committee in February 2017, and the Audit Committee and Board in March 2017. Immediate action was put in place to train key staff in core information governance responsibilities, and to procure expert advice to implement the required improvements.

In March 2017, suppliers were appointed to support improvements in our information governance activities and contracted to December 2017. This proved extremely helpful and this work has been continued into 2018 to provide longer-term strategic improvement advice to the Care Inspectorate, including around planning for the GDPR. This diagram shows the areas of improvement activity that are now underway:



2.0 THE GENERAL DATA PROTECTION REGULATION

From May 2018, the General Data Protection Regulation will enhance the data protection regime across the European Union, and amongst those countries that trade with the EU. The EU regulation will apply UK-wide from May 2018, and will be augmented and described in detail by new primary legislation.

The Data Protection Bill, if given royal assent, will create new domestic legislation, and thus its provisions will not be directly impacted by Brexit.

The GDPR represents an evolution in privacy law and not a revolutionary change. The Care Inspectorate already has privacy arrangements in place to support compliance with the current privacy legislation, so its work to become compliant with new regulation is not starting from scratch. Many of the new mandatory requirements under GDPR are already promoted by the UK Information Commissioner as good practice to support compliance with the current UK Data Protection Act, e.g. privacy impact assessments for major organisational changes. Others represent the formalisation of good business practice and governance, e.g. retention of records as evidence of accountability and compliance.

The GDPR is not enforced until 25 May 2018 and at the time of writing, we are awaiting formal guidance from the UK and EU regulatory bodies for some aspects of the new regulation. With no legal precedents and current gaps in guidance, working towards compliance will continue well beyond May next year for all organisations across the UK, but there are key activities that we must progress now.

Key changes and mandatory requirements include:

- maintaining a personal data register, showing what, why and how personal data is held and processed from point of capture to disposal
- maintaining evidence of accountability and compliance – proving that organisations are doing what they say they are doing
- taking a “privacy by design” approach to organisational change to manage risks associated with those changes which may impact on personal privacy
- mandatory appointment of a data protection officer, including for public authorities
- data processors now have direct obligations under the regulation; this changes the data controller–processor relationship
- individuals have a right to explicit information about why an organisation is processing their data, under what lawful basis, and how it will process it, including how long it will keep it for and who it may share it with; existing data rights in this area are strengthened
- bigger fines and easier redress for individuals for harm caused as a result of data breaches
- mandatory regulator notification for serious data breaches, within 72 hours of awareness.

Appendix 1 provides high-level advice from the UK Information Commissioner’s Officer to organisations about their preparation for the GDPR. More information on the Care Inspectorate’s progress towards meeting these is set out below.

3.0 IMPROVEMENTS IN THE CARE INSPECTORATE'S INFORMATION GOVERNANCE ACTIVITIES

Since our consultants were appointed in March 2017, significant improvements have taken place in our information governance activities. This section provides a summary of these improvements.

- We have put in place training for the Senior Information Risk Owner and commenced training for all Information Asset Owners. This helps to embed responsibilities for information governance across the senior team, mainstreaming awareness into all of our work.

- We have developed an Information Asset Register, which will show the information held by the Care Inspectorate and the relevant access arrangements. This will be continually populated and developed by Information Asset Owners, and will set out the clear retention periods for different types of data. It will also demonstrate where personal data is held, ensuring compliance with the GDPR on this point. We have commenced the development of a new business classification scheme which will assist in better organisation and storage of Care Inspectorate data.

- A data incident procedure has been agreed by the Executive Team, showing clearly how breaches or potential breaches of data will be managed and consequent risks mitigated as soon as possible. This has been tested on one suspected data breach, which, although it was found to be very minor and not reportable, has helped to test the robustness of the policy. A data breach log is maintained by the information governance team and used to inform organisational quality improvement: for example, as a result of past learning, measures are being put in place to support secure file transfer externally.

- An information risk register has been produced, to align with the Care Inspectorate's corporate risk regime. This is regularly reviewed and helps to identify where risks may present and to ensure they are being managed.

- The Executive Team has agreed a new core record-keeping policy to ensure that records are kept to an appropriate standard, supporting retention, classification, and freedom of information obligations.

- In anticipation of the GDPR, we are building in information governance and privacy requirements to our new business transformation programme, but further work in this area will be needed to adopt a digital by default in the future. We are planning the development of a data protection impact assessment template for organisational developments, which will support GDPR compliance.

- We have completed an initial review of offsite storage of historical paper records. Most are life-expired and should be destroyed. Those that are suitable for destruction have been scheduled for destruction; historical records which are not required by the Care Inspectorate but may be of interest to the Scottish Child Abuse Inquiry will be retained until its conclusion, out of an abundance of caution.

- We have improved how people wanting to make a freedom of information requests or subject access requests can use our website, and highlighted the necessary information about the reuse of public information. We have adopted the model publication scheme published by the Scottish Information Commissioner and have updated and placed online our guide to the information we publish and hold. We have updated our registration entry with the UK Information Commissioner to more comprehensively reflect the work we do. We have improved the functionality and availability of the Care Inspectorate datastore, increasing the amount of self-serve information that can be obtained from the website without the need for making FOI requests.

- We have sought to improve staff awareness and understanding of information governance, including the provision of baseline training to 50 key managers, sessions with the Senior Management Team, and individual briefings with Information Asset Owners. We are continually improving the information available for staff to see on the intranet.

Further work is ongoing in:

- identifying a Care Inspectorate Data Protection Officer
- developing and agreeing a new data protection policy, to implement requirements of the Data Protection Bill once the legislative process if finalised
- agreeing a retention schedule for all data
- publishing core and specific privacy notices, so people know how and why personal information is collected and used
- mapping personal data flows in and out of the Care Inspectorate
- rationalising our computer drives to reflect the new business classification scheme
- planning robust and comprehensive staff training in relation to our new polices and procedures.

Our information governance consultants will support this work during the first half of 2018, as well as specific action planning to prepare for the GDPR. Their strategic advice will focus on policy development, culture change around information governance, compliance with GDPR, improvement of our physical and digital systems for information storage, and risk and performance in information governance.

Further information is provided in Appendix 2 which sets out in detail the GDPR thematic areas which have commenced and the actions that require to be undertaken between January and May 2018, subject to the caveat that the Bill is still progressing its passage.

4.0 RESOURCE IMPLICATIONS

There are significant implications for Care Inspectorate staff to continue the programme of information governance improvement, prepare for the GDPR, and raise organisational understanding and capacity. The costs will be met from existing resources.

5.0 CUSTOMER SERVICE IMPLICATIONS

Information governance excellence will support good customer service, particularly around requests for information and enhanced provision of data and statistics on our website.

6.0 BENEFITS FOR PEOPLE WHO EXPERIENCE CARE

Effective storage and retention of information will help ensure that the Care Inspectorate is operating effectively and to the high standards expected of a public sector organisation. Effective records management will improve our ability to interpret and act on intelligence about care.

7.0 CONCLUSION

The Board is invited to note and discuss this paper.

LIST OF APPENDICES

Appendix 1 - Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now
Appendix 2 - Summary of GDPR themes and implementation progress