AGENDA ITEM NO 6

REPORT NO IJB 18/18

ANGUS HEALTH AND SOCIAL CARE

INTEGRATION JOINT BOARD – 21 FEBRUARY 2018

CHANGES TO STATUTORY INFORMATION GOVERNANCE REQUIREMENTS

REPORT BY VICKY IRONS, CHIEF OFFICER

ABSTRACT

This report aims to raise the awareness of the Integration Joint Board in relation to the General Data Protection (GDPR) Regulations 2016 which come into force on 25 May 2018, supported by the Public Records (Scotland) Act 2011. The report sets out the actions required to comply with requirements of GDPR. It is understood that the Keeper of the National Records of Scotland will require the IJB to prepare and submit a Records Management Plan under the terms of the Public Records (Scotland) Act (PRSA) 2011 at some point during 2018. The report seeks approval from the Joint Board for an action plan to meet these statutory requirements and permission to register the Joint Board as a "data controller" with the Information Commissioner.

1. RECOMMENDATIONS

It is recommended that the Integration Joint Board:

(i) notes the content of the report and the implications for the Joint Board of the Public Records (Scotland) Act 2011 and the General Data Protection Regulations 2016;

(ii) approves the action plan as set out in Appendix 1;

(iii) agrees to register the Joint Board with the Information Commissioner as a "data controller";

(iv) requests that a progress report be submitted to the next meeting of the IJB.

2. THE MANAGEMENT OF PUBLIC RECORDS

2.1 BACKGROUND

Under the Public Records (Scotland) Act 2011 all public bodies in Scotland are required to take appropriate measures to ensure the records of their business are kept appropriately. The Act empowers the Keeper of the National Record of Scotland to require each public body to prepare and submit a Records Management Plan for his approval, setting out the public body's current records management arrangements and their plans for improvement.

Integration Joint Boards (IJBs) are public bodies for the purposes of the Act. The Keeper has indicated all IJBs are to be included in the 2018 cycle for Records Management Plan submissions. No date has yet been published but it is understood that formal invitations to submit are likely to be issued in July or August of this year.

2.1.1 RECORDS MANAGEMENT PLANS

The Keeper has issued a model records management plan for IJBs. The model covers 14 key elements:

1 Senior management responsibility

2 Records manager responsibility

3 Records management policy statement

4 Business classification

5 Retention schedules

6 Destruction arrangements

7 Archiving and transfer arrangements

8 Information Security

9 Data protection

10 Business continuity and vital records

11 Audit trail

12 Competency framework for records management staff

13 Assessment and review

14 Shared Information

The timetable for submission of the records management plan is relatively short. Once the Keeper formally announces his intention to invite the IJB to submit its plan there will be a period of six months until the actual letter of invitation is issued. Once the formal invitation is received the IJB will have four months in which to submit its plan. There will then be a three month period in which the Keeper may seek revisions before the Keeper publishes his final report on the records management plan along with the plan itself.

Although the records of the IJB are not complex, and their volume is small, it will need to prepare a comprehensive records management plan covering all these elements. This will be a resource intensive task as it will require the collection of evidence to support each of the elements and, in some cases, the development of new policies and processes.

The following areas are of particular note.

2.1.2 RECORDS MANAGEMENT RESPONSIBILITY

The IJB will require to appoint a senior manager to undertake the task of responsible officer, overseeing the management of the partnership's records.

Ensuring the proper management, preservation, and archiving of public records is a central aim of the Act. The Act requires that records management be directed by a suitably qualified records manager and that appropriate storage and archiving arrangements are in place.

Given that the IJB is unlikely to produce significant volumes of records in the conduct of its business it may be that it might be most cost effective to delegate the task of records management to either NHS Tayside or Angus Council as part of a revision of the existing support agreement rather than employing a records manager directly.

2.1.3 BUSINESS RECORDS CLASSIFICATION

The partnership currently has no agreed classification system for organising and managing its records. A classification system is more than just a filing system: it describes the different aspects of the business of the IJB, and how they relate to each other and the records produced in the course of conducting each area of business.

NHS Tayside and Angus Council have already submitted their record management plans and are in the course of implementing them. Both bodies are introducing business classification

schemes and it will be important that the IJB adopts a scheme which is broadly in line with those adopted by its constituting partners.

Part of that process will be to compile an information asset register covering all information produced or held by the IJB.

2.1.4 INFORMATION SHARING ARRANGEMENTS

The records management plan will require to include evidence of robust information sharing arrangements covering not only data sharing between NHS Tayside and Angus Council, but between those bodies and the IJB as well as local organisations, providers and national agencies such as NHS National Services Scotland.

These arrangements will need to reflect both the provisions of the Public Bodies (Joint Working) (Scotland) Act 2014 and the General Data Protection Regulations 2016.

2.2 CURRENT POSITION

The IJB does not currently have a designated senior manager responsible for records management. The IJB does not have agreed arrangements in place in respect of elements 2 to 13 of the records management plan model.

As part of the implementation of Angus Council's wider records management plan, retention and deletion policies are been reviewed, a new secure archiving and scanning facility is being established, and the local government business classification scheme is being implemented for all records, including personal records. Staff within the partnership's Improvement and Development Team have been leading on this work within adult care services to ensure this work is completed in a way which is fit for the purposes of the partnership.

As part of this work the improvement and development team have commenced compiling an information asset register and drafting a business classification scheme for IJB records, based on the Local Authorities Business Classification Scheme adopted by Angus Council.

It should be noted that NHS Tayside is at an earlier stage of implementing its records management plan and is still in the process of developing a business classification scheme. NHS Tayside has not yet issued guidance to services or to the IJB regarding implementation of their records management plan. NHS Tayside has a national meeting in May to discuss GDPR, to which representatives from Legal Services in Angus Council have been invited. Once guidance is received a further paper will be submitted to the IJB for consideration.

Information sharing between NHS Tayside and Angus Council is currently governed by a data sharing agreement made in 2007.

The data sharing agreement is no longer fit for purpose. It reflects partnership arrangements which have been superseded by the Public Bodies (Joint Working) (Scotland) Act 2014. It is not consistent with the "gold standard" model set out in the Scottish Government Information Sharing Toolkit 2016, nor is it consistent with the requirements of the PRSA or the GDPR.

The agreement urgently needs to be fully revised and re-negotiated with NHS Tayside, Tayside Local Authorities, and the other Tayside IJBs. Achieving such an update is being actively pursued.

3. THE PROTECTION OF PERSONAL INFORMATION

3.1 BACKGROUND

Personal information about individuals held by organisations in the UK is subject to protection under the Data Protection Act 1998.

In 2016 the European Union agreed a revised set of regulations – the General Data Protection Regulations 2016 (GDPR) – which extends the rights of individuals over their personal data, expands the duties of organisations which control or process personal information, and introduce heavier financial penalties for breach of the regulations.

The GDPR comes into force on 25 May 2018. The UK Government has decided that the GDPR will be incorporated permanently into UK law and a new Data Protection Bill enacting the GDPR is currently proceeding through the UK Parliament.

The UK Information Commissioner is responsible for regulation and enforcement of the GDPR and the Data Protection Act.

Under the GDPR the IJB is required, as a public body, to appoint a data protection officer.

3.1.1 RIGHTS OF DATA SUBJECTS UNDER THE GDPR

The GDPR gives individuals greater rights over personal data held about them than they have under the existing Data Protection Act. Under the GDPR data subjects have the following rights:

- The right to be informed about what information is being collected and how it is processed
- The right of access to information held about them and how it has been processed
- The right to rectification of any errors in the information held about them
- The right to have records erased (sometimes referred to as 'the right to be forgotten')
- The right to restrict processing of information held about them
- The right to data portability: to be able to have all data transferred to them to enable them to pass it to another provider if relevant
- The right to object to the information held about them or how it is being processed
- Special rights in relation to automated decision making and profiling.

3.1.2 CONSENT AND OTHER LEGAL GROUNDS FOR PROCESSING

The extent of these rights in each case is dependent upon the legal basis on which the information has been collected and processed. There are five relevant legal bases available to public bodies under the GDPR:

a) Consent of the data subject
b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
c) Processing is necessary for compliance with a legal obligation
d) Processing is necessary to protect the vital interests of a data subject or another person
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

'Consent' confers the most extensive rights on the data subject and gives the individual the greatest control over what is done with their personal information. However, the GDPR sets high standards for what counts as 'consent'. It requires that explicit consent is obtained from the data subject for each specific data processing action including data sharing, and in relation to every person who has access to their information. This would be impractical in the complex health and social care context. The GDPR also requires that the 'consent' is based on a real choice, where it is a realistic option for the data subject to refuse to share their information or for it to be processed in some way. In particular, under the GDPR it is unlikely that 'consent' could be used as a basis for lawful processing where there is an asymmetrical power relationship between the data subject and the organisation processing the data, for example, a public authority.

The Information Commissioner has issued statutory guidance that 'consent' is generally not the most appropriate basis for public authorities to process personal data and that the other four bases listed above are more likely to provide a secure legal basis for processing under the GDPR. Typically, the collection and processing of personal information in the course of carrying out of the functions delegated to the IJB will be done under (d) or (e) above. In cases where services are provided under contract by third parties such as care homes, (b) will be the most relevant basis for processing while in relation to the protection of vulnerable adults or the prevention of fraud, (c) offers the most secure legal basis for processing.

It is worth noting that under section 49 of the Public Bodies (Joint Working) (Scotland) Act 2014, NHS Tayside, Angus Council, and the Angus IJB may share any individual personal data in the course of carrying out the functions delegated to the IJB irrespective of any duty of confidentiality to the individual. Such data sharing does not require the data subject's consent.

The Data Protection Act 1998 requires 'data controllers' to inform data subjects about how their personal information is processed and their rights under the Act through publication of privacy notices. Privacy notices under the GDPR require to be more detailed. They need to specify the legal basis for processing, the name and contact details of the 'data controller', the purpose of the processing, the type of processing which will be carried out, who data will be shared with, how the security of the data will be ensured, and the extended rights of the data subject over their personal data.

3.1.3 THE ROLE AND DUTIES OF DATA CONTROLLERS

The GDPR places special duties upon 'data controllers'. It defines a 'data controller' as '*… the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data …'* (Article 4(7)).

Angus IJB collects and uses personal information about a range of individuals including members of the board, staff within NHS Tayside and Angus Council, staff and committee members of other organisations, service users, carers, and other members of the public. It does so in order to carry out its integration functions including public engagement, strategic planning, information sharing, and governance. On this basis Angus IJB is a 'data controller' under the GDPR.

While the IJB does not itself collect or use personal information for the carrying out of health and social care functions, under sections 25 and 26 of the Public Bodies (Joint Working) (Scotland) Act 2014 it does have all the powers and duties of those delegated functions and is required to direct the 'constituent authorities' (i.e. NHS Tayside and Angus Council) as to how they are to carry out those functions. As such direction may include the collection of personal information in carrying out those functions, the IJB may also be a joint 'data controller' in respect of personal information collected and used by the 'constituent authorities' in carrying out those functions.

As a 'data controller' the IJB requires to be registered with the Information Commissioner.

Under the regulations the IJB is required to identify every piece of identifiable personal information which they hold on service users, carers, staff, and other individuals. The IJB must be able to show on what legal basis it holds the information, where the information was obtained, what the information is used for, who has access to the information, and who the information is shared with.

For every individual which the IJB holds information about it needs to be able to provide a chronology of every time the information has been accessed, read, amended, processed in any way, used for any purpose, combined with other information, shared, archived, or deleted, and who has carried out these actions.

3.1.4 PENALTIES FOR BREACHES OF THE GDPR

The GDPR reduces the deadline for responding to requests from individual exercising their rights as data subjects from 40 days to one month. The regulations also require that any serious data breach must be reported to the Information Commissioner within 72 hours.

Breaches under the regulations can attract civil penalties of up to €20m per breach, unlimited civil compensation to the data subjects affected and, in some cases, criminal proceedings. Failure to notify the Information Commissioner of a serious breach within 72 hours can result in civil penalties of €10m. Fines are in Euros, reflecting the fact that the legislation is pan-European.

The IJB will require to have robust processes in place to identify breaches of the regulations and to respond to requests from those individuals it holds information about to amend or delete their information or to make complaints regarding the use or abuse of that information by us or people we have shared the information with. In so far as the IJB is 'joint data controller' of personal data collected in the carrying out of its delegated functions, the IJB will need to be assured that retention and destruction policies are rigidly applied.

3.2 CURRENT POSITION

The IJB is not currently registered with the Information Commissioner as a 'data controller' as will be required under the GDPR.

Angus Council has established a number of working groups to implement the GDPR across all its functions including Adult Care. An Information Asset Register has been collated covering all personal information held by the council, whether as a 'data controller' or a 'data processor', and has begun the process of revising its privacy notices. Staff within the partnership's improvement and development team have led this work as it relates to the carrying out of functions delegated to the IJB.

NHS Tayside is at an earlier stage in in its preparations to implement the GDPR. At this stage NHS Tayside has not issued guidance to services or to the IJB on the steps that need to be taken to comply with the regulations before they come into force on 25 May 2018. Once guidance has been received from NHS Tayside a further report will be submitted to the IJB in this regard.

The IJB, NHS Tayside and Angus Council do not currently have robust systems to ensure that copies of personal information are effectively limited and secured. While information held on management information systems such as MiDiS, Vision, or CareFirst are secure and log all instances of access to individual records, paper systems and electronic filing on shared drives are not well controlled. In particular, mailing lists, copies of letters and emails, and various ad hoc spreadsheets and databases are often retained by staff on shared drives, and there is no systematic process in place to ensure access to them is monitored and that they are deleted in line with retention and disposal policies.

In order to comply with the GDPR it will be necessary to audit all duplicate personal information held and destroy all copies which are not immediately required for legitimate processing purposes. This is to ensure that if asked by a data subject we can specify all instances of information held on them, can ensure all copies are correct and up to date, and can ensure access to that information is controlled and lawful. Without undertaking this data cleansing and consolidation action it will be extremely difficult to limit to opportunities for data breaches to occur.

Angus Council is establishing a secure data storage facility for paper records which are within their retention period but no longer active. The storage area will also have facilities for digitising paper records for consolidation with electronic records within a secure document management system. This will enable a transition from the current mixed media system where an individual's adult care records may be split over several paper and electronic systems, to a secure electronic based single record for each individual.

The IJB may wish to consider a similar approach in respect of personal information records held by the IJB.

4. PROPOSALS

Appendix 1 sets out an action plan for implementation of the GDPR and for preparing a records management plan for submission by the IJB.

The IJB is asked to approve the proposed action plan. The IJB is also asked to agree to item 1 of the action plan, that the IJB be registered as a 'data controller' with the Information Commissioner before the commencement of the GDPR.

A progress report will be submitted to the next meeting of the IJB in relation to item 2 of the action plan regarding the appointment of officers to undertake the roles of Senior Responsible

Manager and Data Protection Officer, and the appointment of a suitably qualified officer or contractor as Records Manager.

A further report will be submitted to the IJB regarding implementation of the GDPR in respect of NHS delegated functions once guidance has been received from NHS Tayside.

5. FINANCIAL IMPLICATIONS

The work outlined in Appendix 1 will involve significant staff resources over the next 12 months. It will also require the appointment of a Data Protection Officer and either the appointment of a suitably qualified Records Manager or the procurement of such a service from a partner body or external party.

At this stage it is not possible to quantify whether there will be any additional costs arising from the action plan, and if so the scale of such costs. The report will be submitted to a future meeting of the IJB, providing estimates of the short and medium term costs arising from the action plan in Appendix.1 once these become clearer.

REPORT AUTHOR: George Bowie, Head of Community Health & Care Services (South Angus)
Gail Smith, head of Community Health & Care Services (North Angus)

EMAIL DETAILS: BowieGS@Angus.gov.uk
gailsmith@nhs.net

List of Appendices:

1. Information Governance Action Plan

APPENDIX 1: INFORMATION GOVERNANCE ACTION PLAN

Action	Target Date End of:	Responsible	Legislation Implemented		Functions Affected	
			PRSA	GDPR	IJB Business	Council Delegated
1. Register IJB as a Data Controller	April 2018	IJB		✓	✓	✓
2. Appointment of Responsible Officers / Contractors						
Senior Manager to Oversee Records Management	April 2018	IJB	✓		✓	
Records Manager / Contractor	April 2018	IJB	✓		✓	
Data Protection Officer	April 2018	IJB		✓	✓	
3. Compile Information Asset Register						
Personal Data (Adult Care)	January 2018	Admin	✓	✓		✓
Personal Data (IJB)	February 2018	Admin	✓	✓	✓	
Non-Personal Data	June 2018	Admin	✓		✓	✓
4. Design and Implement Business Classification Scheme						
Personal Data	March 2018	IDT / Admin /IT	✓	✓	✓	✓
Non-Personal Data	September 2018	IDT / Admin /IT	✓		✓	✓
5. Review and Revise Privacy Notices	April 2018	IDT / Admin /IT		✓	✓	✓
6. Revise and Agree New Data Sharing Agreement	25 May 2018	NHS Tayside / Tayside IJBs / Tayside Councils	✓	✓	✓	✓
7. Agree Retention Schedules	April 2018	R2	✓	✓	✓	
8. Agree Destruction Arrangements	April 2018	R2	✓	✓	✓	

Action	Target Date End of:	Responsible	Legislation Implemented		Functions Affected	
			PRSA	GDPR	IJB Business	Council Delegated
9. Data Cleansing and Consolidation						
Personal Data	25 May 2018	Admin / All Staff	✓	✓	✓	✓
Non-Personal Data	September 2018	Admin / All Staff	✓		✓	✓
10. Design and Implement Information Access Audit System						
Personal Information	25 May 2018	IDT / Admin / IT	✓	✓	✓	✓
Non-Personal Information	September 2018	IDT / Admin / IT	✓	✓	✓	✓
11. Review of Information Security Arrangements	September 2018	IDT / RM / Admin / IT	✓	✓	✓	✓
12. Records Management Plan						
Prepare Draft Plan	September 2018	IDT / RM	✓		✓	
Collate Supporting Evidence	September 2018	IDT / RM	✓		✓	
Approve Final Plan for Submission	October 2018	IJB	✓		✓	

Key
IDT: Improvement and Development Team
IJB: Integration Joint Board
IT: Angus Council IT Division
R2: Angus Partnership Clinical and Care Governance Group
RM: Records Manager / Contractor