EXPLANATORY MEMORANDUM TO

THE DATA PROTECTION (ASSESSMENT NOTICES) (DESIGNATION OF NATIONAL HEALTH SERVICE BODIES) ORDER 2014

2014 No. 3282

1. This explanatory memorandum has been prepared by the Ministry of Justice (MoJ) and is laid before parliament by command of Her Majesty.

2. Purpose of the instrument

2.1 The purpose of the instrument is to designate traditional public sector providers of NHS services for the purposes of section 41A DPA. These providers are listed in Schedule 1 part 3 of the Freedom of Information Act 2000, and Schedule 1 part 4 of the Freedom of Information (Scotland) Act 2002. This will extend the Information Commissioner's ("the Commissioner") powers of compulsory audit to public sector NHS bodies to enable him to assess whether they are complying with the data protection principles under the DPA.

3. Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None.

4. Legislative Context

4.1 Section 41A of the DPA provides that the Commissioner may serve designated data controllers with an assessment notice for the purpose of enabling the Commissioner to determine whether they are complying with the data protection principles contained within the DPA. An assessment notice, given with reasonable notice, allows the Commissioner, for example, to enter and inspect premises, inspect certain documents or equipment and permit the interview of staff for the purposes of carrying out a compliance audit.

4.2 Government departments are automatically covered by the assessment notice scheme by virtue of section 41A(2)(a). Wider public authorities can be made subject to the power by being designated for the purposes of the scheme by an order made under section 41A(2)(b). According to section 1(1) of the DPA a "public authority" means a public authority within the Freedom of Information Act 2000 (FOIA) or a Scottish public authority within the Freedom of Information (Scotland) Act 2002 (FOISA). Additionally, section 41A(12) adds that public authority may also include any body, office-holder or other person in respect of which an order may be made under section 4 or 5 FOIA or under section 4 or 5 FOISA. Only the section 1(1) limb is material for the purposes of this Order.

4.3 This Order is made under section 41A(2)(b) and designates "traditional" public sector providers of NHS services listed in Schedule 1 part 3 FOIA and Schedule 1 part 4 FOISA, as well as the Health and Social Care Information Centre listed in Schedule 1, part 6 FOIA.

5. Territorial Extent and Application

5.1 This instrument applies to all of the United Kingdom.

6. European Convention on Human Rights

6.1 The Minister of State for Justice has made the following statement regarding Human Rights:

In my view the provisions of the Data Protection (Assessment Notices) Designation of National Health Service Bodies) Order 2014 are compatible with the Convention rights.

7. Policy background

7.1 The Order will designate NHS bodies and is intended to improve the monitoring of their compliance with data protection law; to provide a stronger incentive for them to agree to consensual audits by the ICO and to improve public confidence in the protection of their personal data.

7.2 In 2011, the Commissioner submitted a business case to the Ministry of Justice requesting that the Secretary of State use the Order-making power under section 41A (2)(b) DPA to extend the Commissioner's powers of compulsory assessment of compliance with the DPA's data protection principles. The Commissioner requested that these powers be extended to allow it to assess public sector NHS bodies. The evidence provided in the business case demonstrated that the NHS was an area within which the use of assessment notices would be beneficial.

7.3 The main factors upon which the Commissioner based his recommendations were:

- The sector processes large amounts of sensitive personal data;
- The Commissioner receives a high number of complaints and self-reported breaches of the DPA by NHS bodies;
- The Commissioner's Good Practice team have identified many examples of significant risks to individuals' personal data in its consensual audits of the NHS;
- The number of consensual audits of NHS bodies (53%) is significantly below the average across the public sector as a whole (71%).

7.4 Based on the evidence presented by the Commissioner in his business case and the responses from NHS bodies and others to the consultation document, the government believes a compelling case has been made for extending the Commissioner's powers of compulsory audit to public authority NHS bodies. The Government believes the benefits include:

- Encouraging NHS bodies to improve their compliance with the data protection framework.
- Incentivising NHS data controllers to sign up to consensual audits.
- Improving public confidence in regards to the protection of sensitive personal data by NHS bodies.

7.5 The range of public authority NHS bodies which are being designated will reflect the "traditional" public sector providers of NHS services listed in Schedule 1 part III of the Freedom of Information Act 2000, and Schedule 1 part 4 of the Freedom of Information (Scotland) Act 2002. In practical terms, this includes Foundation Trusts, GP Practices, Clinical commissioning groups but not contracted private and third party sector bodies providing NHS services such as pharmacies, opticians and dentists.

7.6 Extending to private or third sector providers of NHS services would require a separate consultation and Order under s.41(2)(c) of the DPA. We will continue to work with the Information Commissioner to keep this under review. It should however be noted that s.51 (7) DPA contains provisions giving the Information Commissioner powers to assess any organisation's processing of personal data for the following of 'good practice' with the agreement of the data controller, including private and third sector providers of NHS services. These bodies are also required to comply with the data protection principles in the DPA when handling personal data.

7.7 As outlined in his *Assessment Notice code of practice,* the Commissioner sees auditing as a constructive process with real benefits for data controllers and data subjects alike and so aims to establish, wherever possible, a participative approach. In doing so he has indicated that his power to serve an assessment notice is very much a backstop and that his preference is for organisations to volunteer for consensual audits in the first instance unless the circumstances make this inappropriate.

8. Consultation outcome

8.1 An informal consultation, entitled, 'Assessment notices under the Data Protection Act 1998: extension of the Information Commissioner's Powers' was launched by the MoJ and ran between 25 March 2013 and 17 May 2013. There were 76 responses to the consultation. The majority of responses (88% of total responses and 93% of NHS bodies who responded) were in favour of the proposal to extend the Commissioner's assessment notice powers to NHS bodies.

8.2 In summary, those in favour were of the view that the proposal was justified because data protection compliance was generally low in NHS bodies. Most respondents felt assessment notice powers were an important tool for the Commissioner in driving up compliance and would encourage NHS bodies to opt for consensual audits so that risk areas could be identified and addressed before problems arise.

8.3 Those respondents opposed to the proposal were of the view that the audits would be too onerous and consequently place additional burdens on an already heavily regulated sector. Others were concerned that there were no plans to allow compulsory audits in other public service sectors where breaches of data protection law were prevalent.

8.4 On 15 July 2014, the Government published its response to the consultation. In light of the responses received and of the strong evidence of significant and widespread data protection compliance concerns within the NHS, the response set out the Government's intention to lay an Order designating traditional public sector NHS bodies under section 41A of the DPA.

8.5 Both the consultation paper and response can be found on the MoJ website at: https://consult.justice.gov.uk/digital-communications/ico-assessment-notices

9. Guidance

9.1 As required by section 41C of the DPA, the Commissioner has prepared and issued a Code of Practice to address how his functions in connection with assessment notices will be exercised. This Code is available on the Commissioner's website.
https://ico.org.uk/what_we_cover/taking_action/~/media/documents/library/Corporate/Detailed_specialist_guides/assessment_notices_code_of_practice_2012.pdf

10. Impact

10.1 There are no specific impacts on business, charities and voluntary bodies as the measure only applies to traditional public sector NHS bodies.

10.2 The Impact on the Public Sector and in particular NHS bodies is likely to be positive. The Government believes the benefits are:

- Encouraging NHS bodies to improve their compliance with the data protection framework.
- Incentivising NHS data controllers to sign up to consensual audits.
- Improving public confidence in regards to the protection of sensitive personal data by NHS bodies.

10.3 An Impact Assessment has not been prepared for this instrument. The impact is limited to the public sector and the annual impact will be significantly below the £5 million threshold for requiring an impact assessment.

11. Regulating small business

11.1 The legislation does not apply to small business.

12. Monitoring & review

12.1 The Government will continue to work closely with the Commissioner to ensure he has adequate powers to enforce compliance with the DPA by organisations that handle personal data. This includes keeping under review whether it might be appropriate at some point in the future to make an order under s.41A(2)(c) of the DPA which would extend the ICO's powers of compulsory audit to private and third sector contractors of NHS services.

13. Contact

Amanda Williams at the Ministry of Justice Tel: 020 3334 3915 or email: amanda.williams@justice.gsi.gov.uk can answer any queries regarding the instrument.