



Information Commissioner's Office

## **Response from the Information Commissioner's Office to the Maternity Strategy for Northern Ireland consultation document**

### **Introduction**

The Information Commissioner ('the Commissioner') has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 ('DPA') and the Freedom of Information Act 2000 (FOIA). The Information Commissioner's Office ('ICO') is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

The Commissioner's response to this consultation is primarily based on the practical experience gained in ensuring compliance with the information access regimes his office regulates.

### **Background**

The Commissioner welcomes the opportunity to input into this maternity strategy consultation ('the consultation ') issued on behalf of the Department of Health, Social Services and Public Safety ('the Department'). Many of the proposals within this consultation are outside the scope of the work carried out by the Commissioner. For the purposes of this response the Commissioner is focussing on the recommendations within the consultation relating 'Communication and Clinical Leadership' and those recommendations relating to the 'NIMATS IT system'.

### **Communication and Clinical leadership**

The Commissioner notes the recommendation at paragraph 24 of the consultation which states:

"High quality maternity care depends on good communication between professionals, an aspect of significant importance when urgent transfers are required between units and one in which difficulties have been cited in Northern Ireland and the United Kingdom when there have been serious adverse incidents in care. All units have now introduced the hand held

record therefore co-ordinated regional development of its use should be easier. Each Trust should ensure its maternity service shows good clinical leadership and communication including the use of the hand held records, Labour Ward Forum and other multidisciplinary groups.”

The Commissioner is aware of the practice in Northern Ireland whereby expectant mothers carry a Regional Maternity Hand Held Record throughout their pregnancy<sup>1</sup>. It is the Commissioner understanding that the mother carries this manual record with them until after their child’s birth whereby they return it. This record is updated as the mother attends appointments or transfers between units of a hospital for example with test results or doctors notes. The Commissioner has concerns about the security of these records, particularly with such an onus being placed on the mother at a challenging time to ensure that it is kept complete, no documents are lost from it and it is transferred from point to point within her maternity care regime and would welcome discussions with the Department about this practice..

The Commissioner would draw the Department’s attention to the seventh principle of the DPA<sup>2</sup>. The seventh principle is one of eight such principles of good information handling at the heart of data protection. The main purpose of these principles is to protect the interests of individuals whose personal data is being processed. They apply to everything that an organisation does with personal data, except where it is entitled to an exemption<sup>3</sup>. The seventh principle states:

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

The Commissioner considers that in practice the seventh principle means an organisation must have appropriate security in place to prevent the processing of personal data held being accidentally or deliberately compromised. In particular an organisation will need to:

- design and organise its security to fit the nature of the personal data that it holds and the harm that may result from a security breach;
- be clear about who is responsible for ensuring information security
- make sure the right physical and technical security is in place backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively

---

<sup>1</sup> For further information [http://www.dhsspsni.gov.uk/nmag-maternity\\_hand\\_held\\_notes](http://www.dhsspsni.gov.uk/nmag-maternity_hand_held_notes) This record the Commissioner understands was developed by DHSSPSNI and launched officially by Minister in March 2010.

<sup>2</sup> Eight data Protection Principles are found at Schedule 1 of the DPA

<sup>3</sup> For further information on exemptions within the DPA, see the ‘Guide to Data Protection’ available at [www.ico.gov.uk](http://www.ico.gov.uk)

The maternity record will contain sensitive personal data <sup>4</sup> relating to the health of the mother. When information is 'sensitive' as defined by the DPA, the Act gives it a higher standard of protection as it is likely to be of a private nature. Given this sensitive nature greater care must be taken in deciding what security is appropriate for the information. The Commissioner is not sufficiently versed with the contents of these records or those policies in place governing their usage to provide detailed comment in this consultation about the adequacy of the security measures being adopted. He would very much welcome further engagement with the Department to address his concerns and to ensure that the provisions of the DPA are being met.

### **The IT support system**

The Commissioner has noted paragraph 26 of the consultation which recommends the following:

"The NIMATS system allows recording of a large amount of detail about the woman's past medical and obstetric history and details of her current pregnancy. However the system could be improved. Ease of information entry, ability to access the system in community settings, communication with other health information systems and retrieval of unit level data to support audit and service improvement are all areas where improvement is essential if we are to make best use of the technology available to us. Now that all units have introduced NIMATS, coordinated regional improvement to the system should be undertaken without delay. The NIMATS system should be reviewed and updated to ensure coordinated regional data collection"

The Commissioner understands that the maternity services in Northern Ireland depend upon the existence of and the efficient running on, information from those who use those services. He is equally aware of the volume and often the complexity of the information required for these services to function. Often the ability to match identifying information from several sources will be needed so that the mother/patient gets the best treatment possible. However expectant mothers entrust sensitive information to those who provide their maternity care. They do so in confidence, and have the legitimate expectation that their privacy will be respected, and that their maternity records will be used in an appropriate way to support their healthcare. It is vitally important that technical and physical security arrangements are given primacy in any changes or improvements to the NIMATS system. Once again the seventh principle of the DPA seeks to ensure that the processing is carried out securely. Owing to this the Commissioner considers that it is important to understand that the requirements of the DPA go beyond the way

---

<sup>4</sup> For definition of Sensitive Personal data ' See s 2 DPA'

information is stored or transmitted in this NIMATS system. The seventh data protection principle relates to the security of every aspect of the processing of personal data. The security measures should seek to ensure that:

- only authorised people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority; and
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

Further information on data security and compliance with the seventh principle is available from the Commissioner's 'Guide to Data protection' Available on his website at [www.ico.gov.uk](http://www.ico.gov.uk)

The Commissioner has noted that a part of this recommendation involves '*communication with other health information systems and retrieval of unit level data*'. The Commissioner would welcome further information on what this specifically involves. He would however like to draw the Department's attention to his Data Sharing Code of Practice which he launched in Northern Ireland on the 28 June 2011. This Data Sharing Code covers data sharing in the context of the disclosure of personal data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation (e.g. one arm of the health service with another). The Data Sharing Code will apply to personal information contained within the NIMATS systems if it is being shared. However, some data sharing does not involve personal data, for example where only statistics that cannot identify anyone are being shared. Neither the DPA, nor the data sharing code, apply to that type of sharing.

The Data Sharing Code is a statutory code which means that it has been approved by the Secretary of State and laid before Parliament. Although it is not legally binding, it adds details and guidance around how to interpret the 'bare minimum requirements' of the DPA in this area. The Data Sharing Code can however be used in evidence in any legal proceedings, not just proceedings under the DPA. The approach suggested is therefore recommended practice but, if not followed, organisations are likely to face criticism and harsher sanctions if any relevant DPA breach is considered by the ICO or the courts<sup>5</sup>.

The Commissioner considers that any organisation who is involved in the sharing of personal data should use his data sharing code to help them

---

<sup>5</sup> S 52E DPA 'Effect of data-sharing code'

understand how to adopt good practice. Adopting the good practice recommendations of the data sharing code will help to ensure that any sharing of personal information is undertaken in a manner that is fair, transparent and in line with the rights and expectations of the people whose information is being shared. The Commissioner has outlined a brief summary of the key features of the new data sharing code for the benefit of this consultation response.

The Commissioner advises that before sharing any personal data, organisations will need to consider all the legal implications of doing so. The ability to share information is subject to a number of legal constraints which go beyond the requirements of the DPA such as the common law test of confidentiality.<sup>6</sup> If an organisation or individual wishes to share information with another person, whether by way of a one-off disclosure or as part of a large-scale data sharing arrangement, they will need to consider whether they have the legal power or ability to do so. The Commissioner's Data Sharing Code has further guidance on the law in relation to data sharing.

### **Factors to be taken into account before sharing personal information.**

The Data Sharing Code lists those factors which should be considered before entering into a data sharing arrangement. To help identify data protection issues, the use of Privacy Impact Assessments is recommended. The Commissioner suggests organisations consider the following questions before sharing any personal information:

- What the sharing is meant to achieve?
- What information needs to be shared?
- Who requires access to the shared personal data?
- When should it be shared?
- How should it be shared?
- What checks can be carried out to ensure the data sharing is achieving its objectives?
- The risks posed by the data sharing.

---

<sup>6</sup> If a party is to be held liable for breach of confidence it must be shown that (1) the material communicated to him had the necessary quality of confidence; (2) it was communicated or became known to him in the circumstances entailing an obligation of confidence; and (3) there was an unauthorised use of that material – See *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41

- Whether objectives could be achieved without sharing the data or by disclosing only anonymous data.
- Whether the organisation will have to amend its data protection notification.
- Whether any of the data will be transferred outside of the EEA.

## **Conclusion**

The Commissioner has welcomed the opportunity to input into this consultation. The Commissioner has indicated that he would be like to engage further with the Department on those areas of the consultation he has considered. The Commissioner is also happy to provide any clarification or further assistance on any of the issues he has raised in the above response.