



Information Commissioner's Office

## **Consultation Liberating the NHS: An Information Revolution The Information Commissioner's response**

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA). He is independent from government and upholds 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 Information Commissioner's Office (ICO) welcomes the opportunity to respond to this consultation. In the response we shall focus on issues that have transparency, data protection and privacy implications.

### **General comments**

The focus on the importance of information in the reformed NHS is borne out by the proposals set out in this consultation paper. In particular we welcome the aim of developing clear record keeping standards along with a body of well trained information professionals. These developments can only be of benefit in helping NHS organisations to comply with the DPA and the FOIA.

While there are a number of developments which we welcome in principle, we would like to see more detail about the proposals beyond that set out in the consultation paper. At the moment the material that has been produced in this and earlier consultation papers has been at a high level. This has provided an indication of the direction the NHS is going to go in but there has been little detail about the practical, implementation of these initiatives. It is important that when these details are being developed there is an opportunity to be involved in this process or at the very least have a chance to comment on the proposals before implementation.

There is one issue which is not specifically covered in the consultation paper. We consider that in order to ensure high levels of transparency in the reformed NHS, all organisations providing

NHS services should be designated as “public authorities” as defined by the FOIA. This would make such bodies subject to the requirements of the legislation. In turn such an obligation will aid the strong wish to establish an NHS with the concept of transparency at its heart.

## **Consultation questions**

Q8 – Please indicate any particular issues, including any risks and safeguards, which may be taken into account in sharing records in the ways identified in this consultation document.

A – The ability to easily share records where needed is one that can only be of benefit to both health professionals and patients. There are though risks with this approach. From a data protection perspective this includes;

- possible inappropriate sharing of information,
- general security risks,
- ensuring that the records being shared are accurate and having a system in place that allows inaccuracies, once identified, to be corrected in a straightforward manner,
- the possibility of creating duplicate records which may later become dangerously out of date (because while both the original and duplicate are accessible, only one is updated and hence a record that is not up to date could be accessed and used with potentially significant detriment to the patient because subsequent developments have rendered the original information inaccurate), and
- making a full response to a data protection subject access request difficult because of the existence of many duplicated and unnecessary records.

One safeguard that should be used is the carrying out of a [Privacy Impact Assessment](#) (PIA). This would identify and help develop ways to mitigate risks. The ICO has published a handbook to assist with this process and would provide specific advice if it is requested. A PIA would also be the first step in implementing a "[privacy by design](#)" approach. This is where privacy and data protection compliance is designed into systems holding information right from the start, rather than being bolted on afterwards or ignored.

It is also essential that in order to mitigate risks clear standards need to be set and specific NHS guidance needs to be provided about sharing records. Material for this approach could be drawn

from the existing ICO [Framework code of practice for sharing personal information](#).

Within the next few months this code will be replaced when the ICO publishes a new Data Sharing Code of Practice. This will be a statutory code brought in under the provisions of the Coroners and Justice Act 2009. It will set out relevant considerations that will need to be addressed in practice.

Q9 – What kinds of information and help would ensure that patients and service users are adequately supported when stressed and anxious?

A – From a transparency perspective such information and help should be very clear and accessible. There can be nothing worse in such situations than where help is available but there is a bureaucratic, over-complicated and slow way of accessing such assistance.

Q18 – What are your views on the approach being taken and the criteria being used to review central data collections?

Where such collections involve personal data (and more than likely where healthcare is concerned it will include sensitive personal data) steps need to be taken to ensure such collections comply with the data protection principles. Undertaking a PIA will help ensure that this is the case. It will also help identify opportunities to ensure that the information systems themselves contain the necessary features and safeguards and adopt a 'privacy by design' approach.

Q24 – How can health and care organisations develop an information culture and capabilities so that staff at all levels and of all disciplines recognise their personal responsibility for data?

To have an effective information culture an organisation needs to be made good information handling practice very much a "business as usual" application. This means that it is not seen as some burdensome bolt-on extra which has to be complied with, rather good information practice needs to be built into the very way an organisation operates. Usually this is difficult to do with a well established organisation with a set way of working. However the proposed reforms to the NHS in England will see the establishment of new organisations. This in turn provides an opportunity to ensure good information practices become embedded in the way that these

operate. If this is done successfully, while not the complete answer, it will significantly help health and care organisations develop a positive information culture. The methodical use of privacy impact assessments will help reinforce with staff the need for care when personal information is being handled.

The leadership of an organisation has an important role to play in setting the organisation's culture. The ICO has developed the [Personal Information Promise](#) by which leaders commit their organisation to looking after personal information and to report on progress. A number of bodies from the health sector have signed this Promise as an indication of their commitment to looking after the personal information entrusted to them. This approach could be expanded to ensure that all organisations in the health sector (new or existing) show the same level of leadership commitment in this important area.

Q27 – What are the key priorities for the development of professional information management capacity and capability to enable the information revolution?

From the ICO's perspective it is important that there is an approach, which while recognising the importance of data to the NHS, also recognises the importance of transparency and the protection of personal data. It is hard to envisage a successful information revolution without this underpinning.

Q32 – Are there other datasets that you think could be released as an early priority without compromising individuals' confidentiality? Would there be any risks associated with their release – if so, how could these be managed?

As such datasets are likely to contain sensitive personal data it is vital that that when information is released individual confidentiality is maintained. If it is not then this is likely to mean that the data protection principles have not been complied with. The Information Commissioner has powers to serve an Enforcement Notice to ensure future compliance. Depending on the circumstances of such a situation the Commissioner does have further powers to levy an administrative punishment in the form of a Monetary Penalty Notice for up to £500,000.

## **Other issues**

P11, para 1.6 – the involvement of local government in delivering public health does have many potential benefits. However a major concern is whether equally high standards will be adopted by all parties now handling health related information. NHS institutions are familiar with the need to maintain patient confidentiality. If local government is to play a larger role in delivering public health then their management of health related data needs to be done to the same standard as the health service.

In addition while there have been a number of security breaches involving NHS bodies, one reason that the ICO is aware of these is that health organisations are mandated to report them to us. There is no such obligation on local authorities. We consider that there should be a consistent approach adopted by all involved in processing health related sensitive personal data and all such breaches should reported to the ICO.

P17, para 2.5 – we are pleased that the limits of patient/user control of their own records is made clear.

P18, para 2.7 – as set out in the consultation there are potentially significant benefits from increasing patient control over their records. However there are concerns about this control being abused, not by the individuals themselves but by third parties seeking to exploit this control for their own purposes. This could range from attempting to sell unnecessary services to organisations using this information to profile individuals, for example in connection with offering employment or providing insurance services or bank loans. Consideration needs to be given to whether additional sanctions are necessary to help ensure that this is not the case.

P20, para 2.13 – we welcome the emphasis being placed on the necessity of having comprehensive and professionally assured record keeping standards. We consider that having and adhering to such standards will only assist organisations within the reformed NHS to meet their data protection and freedom of information obligations.

P29, para 3.3 and para 3.4 – Quality Accounts – we welcome the development of these reports and think that where providers of NHS healthcare are public authorities as defined by the FOIA then they should be mandated to publish their Quality Accounts through the authority's publication scheme. We also welcome the idea that

Quality Accounts should evolve over time promoting common standards and allowing better local scrutiny.

P39, para 4.17 – the proposal for developing industry recognised competence frameworks to help develop skilled informatics professionals will help to ensure that the NHS keeps a high standard of record keeping.

P41, section 5 – the concept of producing information to hold NHS organisations to account and embedding a “presumption of openness” is another development which we welcome as it fits well with the intentions of the FOIA.

P55, para 6.25 – mandating the adoption of the NHS Number will help with accurate identification of patient information where it is held by different organisations. However we are keen to ensure the uses that the NHS Number can be put to are strictly limited and controlled. We do not want to see a similar situation develop to that which occurred with the National Insurance Number (NINO) where at one stage there were millions more numbers in existence than there were people resident in the UK.

If the NHS Number is to become the unique identifier for patient information it needs to be well managed and subject to strict safeguards. For example after people die and their number becomes redundant then the number should be removed from the system at the earliest opportunity.

The DPA provides that where an identifier is of general application then it can be designated in an order under the Act ([Schedule 1, Part II \(4\)\(1\)](#)) which would include additional safeguards to protect individuals. The increased currency of the NHS number will mean that there is a strong argument for it to be designated and additional safeguards specified.

January 2011