The Information Commissioner's response to the Department of Health's consultation on Protecting Health and Care Information

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000, the Environmental Information Regulations and the Privacy and Electronic Communications Regulations. 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 comment on the Department's proposals to introduce new regulations. As a number of the specific consultation questions relate to areas outside the ICO's regulatory remit, this response answers the specific consultation questions only where appropriate, with the addition of some general points.

Part 1 Introduction

The term "purposes other than direct care" is used in the consultation document. A number of examples of these purposes are referred to in the document such as commissioning and understanding population health needs. Will the regulations specify the "other" purposes? Whatever the "other" purposes are, we would agree that it is vital to ensure that the minimum necessary level of identifiable information is used to fulfil those purposes, and that there is a clear lawful basis for any use of identifiable information, including any sharing that takes place.

We would also agree that robust controls must be in place, but we would suggest that these should exist not only to prevent security breaches and the misuse of information, but to prevent any breach of the DPA.

The general aim over the medium term that access to data will become more automated and, as a consequence, routine functions will no longer require access to identifiable data is one we would welcome.

We also note the reference to using consent more widely as the means to share information. If this is the case we would want to ensure that the subject of consent is approached in a way which is compatible with how the DPA deals with the issue. This is particularly the case where the data to be shared is classed as sensitive personal data (which will be the case for most if not all personal data generated by the health service). In such cases the provision of consent by an individual has to be explicit. If explicit agreement is not obtained or the request for consent is ignored then the proposed processing cannot go ahead.

We are pleased to see the inclusion of proposals for new regulations to address concerns about restrictions on the sharing of confidential personal information with those in the NHS and social care who need to have access to the information in relation to those for whom they are responsible for arranging health or case services. We would comment though that the term "case managers" seems very specific and we would encourage careful consideration to ensure that those who need data for these purposes are able to lawfully obtain it.

We note that the regulations are expected to be in place by the end of 2014 and would comment that this is a tight timescale.

We welcome the focus in paragraph 9 on the importance of clarity around the information shared, and the safeguards in place. We would add that it is also important to set out what information is being processed, and why, as well as how it will be used and by whom, and that a privacy impact assessment may assist in ascertaining this at the outset, as well as identifying the privacy risks and prompting the consideration of ways to mitigate them. Our Conducting privacy impact assessments code of practice[1] may be of use here.

We also note that the proposed regulations would apply in England only. The question therefore arises as to how cross border issues will be addressed.

Part 2 Accredited Safe Havens

This section contains a reference to organisations not sharing information without a clear statutory basis because of the risk of breaching confidentiality law. For public sector organisations we would point out that it there is not a clear lawful basis for processing personal data then this will also be a breach of the first principle of the DPA (which requires that all processing of personal data to be done lawfully).

[1] ICO Conducting privacy impact assessments code of practice

The development of ASHs in order to provide a secure environment to lawfully process identifiable data for a limited range of approved purposes under strict controls is to be welcomed. We would comment that it will be important at the outset to establish which organisations are data controllers and which are data processors in these relationships in order to clarify the data protection responsibilities of the bodies involved.

As the data used by ASHs will be person-level data it is likely to constitute personal data as defined by the DPA, which means that any processing carried out must be in accordance with the DPA (though please see our comments on pseudonymisation and anonymised data in Part 4). Whether the information provided to ASHs comes from the HSCIC, local providers or any other organisation, in order to comply with the first principle of the DPA it is vital to ensure that comprehensive fair processing information has been provided to the individuals whose data is being processed.

On the suggestion that ASHs should be able to retain data for longitudinal studies, we would comment that the fifth principle of the DPA requires that personal data is not kept for longer than necessary. Section 33 of the DPA allows personal data that is being used for research purposes to be retained indefinitely notwithstanding the fifth principle requirements. However, in order to rely on the exemption real research would have to take place; it is not enough to say that the data may possibly be used for some undefined research at some possible future point. In addition, section 33 can only apply where an ASH is retaining data solely for research purposes; if the data is being retained for other non-research purposes then section 33 cannot be applied.

Question 1

No comment

Question 2

We would welcome restrictions on the use of the data and the proposed statutory controls to be placed on ASHs.

Whilst the overarching control should be the "accreditation" by the accrediting body, which should provide some form of documentation, mark or other proof so that organisations and the public know that they can trust the ASH in question, we would also make a number of further points.

The requirement for ASHs to "make available to the Secretary of State or the Information Commissioner any information they require to assist in the investigation and audit of that processing" where confidential

information is processed would need to be framed carefully in proposals so as not to cause any confusion with the Information Commissioner's existing powers to collect information in connection with the exercise of his functions, and with possible future powers of mandatory audit.

The requirement for ASHs to publish a register of data held by the ASH and any information flowing in and out of it is one we would support but we would add that it should reflect the HSCIC register and produce the data flows showing the purpose for the sharing, together with who, if anyone, the data has been shared with for that purpose.

Finally we would suggest a further control to check the notification and performance of the ASH in relation to the DPA.

Question 3

No comment

Question 4

We would suggest that consideration should be given as to whether only 'public' bodies covered by the Freedom of Information Act 2000 should become an ASH, as they have a duty to be open and transparent.

Question 5

We consider the limit should be set on the basis of how many ASHs can be effectively regulated. In order for the "accredited" status of ASHs to have any meaning, in our view there must be a mechanism for regulating and monitoring them. Ultimately if the ASH does not meet the standards required to be accredited then it should be possible to remove the accredited status so that the relevant organisation cannot carry out work until it is successfully re-accredited.

Part 3 Case Management

The proposal in paragraph 43 that the regulations will require a provider of residential care to provide confidential patient information to a commissioner where a request is made in writing suggests that the section 35 DPA exemption from the non-disclosure provisions where that disclosure is required by or under any enactment might apply.
Although the consultation states that it will not be possible to respect individuals' objections to this use of their information, it should be noted that, depending on the Schedule 2 condition used as a basis for the processing, the section 10 of the DPA gives individuals the right to request that a data controller does not undertake processing likely to cause substantial damage or substantial distress. The data controller is

obliged to respond within 21 days saying whether or not they intend to comply with the individual's request. We also note that the NHS constitution gives a right to object.

Question 6

No comment.

Question 7

The ICO frames this in terms of purposes rather than circumstances. If the Regulations require a provider to share patient information with commissioners then it may be the case that section 35 DPA would apply (exemption from some parts of the DPA for disclosures required by law). However, even though this would provide some exemptions from the DPA, a Schedule 2 and 3 condition would still be required.

Question 8

As mentioned earlier, a control from the ICO's point of view would be compliance with the DPA. Particularly important will be need to address fair processing, both in terms of clearly informing people which of their data will be shared, with whom and why, and in terms of any right to object as mentioned above.

Part 4 Controlling the Release of Data

Paragraphs 53-56 refer to the disclosure of pseudonymised information, which is described in paragraph 53 as "information which, whilst not itself identifying individuals, could potentially enable the identity of individuals to be ascertained." This definition broadly equates with the ICO's own approach in recognising that individual-level data – though stripped of 'real world' identifiers such as names or NHS numbers – is more potentially re-identifiable than say aggregated statistical information. However, in determining whether pseudonymised data is personal data or not – the acid test here – we must revert to the definition of 'personal data' in the DPA itself. The DPA's definition of personal data in based on actual identification or reasonable likelihood of this. We are satisfied that pseudonymised information will not – in itself – identify any individual. However, whether or not identification is *reasonably likely* is a matter of fact in particular cases and depends on such factors as:

- how the pseudonymisation is performed, i.e. whether it is combined with other privacy enhancing techniques,
- whether the pseudonymised data is published or released on a controlled basis, and

- the availability of other information that could facilitate re-identification.

We are confident that if the factors above are addressed properly then it is possible to produce pseudonymised data that is not personal data. Please note though there is some disagreement about this and some would maintain that individual-level pseudonymised data is always personal data – a view we reject as incompatible with UK and European data protection law and that is not borne out by the evidence surrounding re-identification risk.

The ICO's definition of pseudonymised data is in our Anonymisation: managing data protection risk code of practice[2]:

> *"The process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity."*

Our definition views pseudonymisation as an anonymisation technique rather than a presumption of identification. Pseudonymised data is normally made up of individual level records where the unique and direct identifiers have been replaced using a process of generating a different unique reference. We reiterate that whether this data is personal data should be assessed in each case.

If we apply this to the information referenced in paragraphs 53-56, if that information cannot identify individuals and where identification is not reasonably likely then it will be effectively anonymised information and the DPA will not apply to it. However if re-identification is reasonably likely then the information should be treated as personal data under the DPA. It follows then that if the HSCIC will be able to re-identify individuals whose identifiers have been removed from a dataset the HSCIC holds, because the HSCIC holds the key which will enable re-identification then this information is personal data in the hands of the HSCIC. However if this dataset is provided to a third party and they are not provided with the key held by the HSCIC – and do not have access to any other information facilitating re-identification then effectively the third party will have been provided with anonymised information which the DPA does not apply to.

Where an organisation does achieve re-identification - and consequently begins to process personal data – it is difficult to envisage how the processing could comply with the requirements of the DPA – particularly 'fairness' and 'lawfulness'. If it does not then the ICO would be prepared to take the appropriate regulatory action against the organisation or organisations involved.

[2] ICO Anonymisation: managing data protection risk code of practice

Question 9

In general we welcome the controls set out in this section, although we would also like to see more detail. For example, how will the HSCIC or an ASH be prevented from disclosing potentially identifiable information to a third party? How will assurance be provided that information this is not intended to identify individuals is not processed in such a way that individuals could be identified?

Question 10

No comment. The ICO can of course issue monetary penalties in the event of a serious breach of the DPA.

Question 11

As mentioned before we would add controls around the notification, fair processing and performance of an organisation in relation to the DPA.
If you have any questions about this submission or require any further information please contact us.

August 2014