HWE Response to Department of Health Consultation: Protecting Health & Care Information

We appreciate the opportunity to give Healthwatch England's response to the consultation on proposals to protect personal health and social care data.

Healthwatch was formed as part of the 2012 reforms of health and social care that set out the ambition of putting people at the heart of health and social care. There is a local Healthwatch in every local authority area in England and Healthwatch England is the national body. Healthwatch is unique in that its sole purpose is to understand the needs, experiences and concerns of people who use health and social care services and to speak out on their behalf.

Healthwatch England is the national consumer champion for health and social care. Healthwatch England has a particular interest in how the public is involved and consulted on the topic of personal data because the public are concerned with the information held about us, how it is collected, who has permission to use it, the purposes for which it is used, how and when it is disposed.

People should have access to their individual records and be able to change or verify the information held on them. Equally, the public expects timely, clear and effective communication about how personal data is safeguarded.

Summary of response to consultation

Healthwatch recognises that there are significant potential benefits to giving researchers access to patient data, and that sharing information effectively can significantly enhance care delivery. Similarly information shared proportionately, sensitively, and in a timely manner between different organisations involved in a person's care can improve their experience of care and health services. Healthwatch is a strong advocate of the Caldicott principles for the use of patient data by health and social care organisations.

Our network of Local Healthwatch (LHW) has alerted us to many concerns about personal data security and this has informed our work to date in this area. In October 2013 prior to the start of the care.data programme Healthwatch Derbyshire used the network's formal procedure for escalating concerns to draw attention to problems around patient anonymity and data sharing. Then in January 2014 Healthwatch Herefordshire raised specific concerns on the proposed roll out of the care.data programme. Healthwatch England consulted the rest of the network and found that one in four Local Healthwatch organisations shared the concern before it became a popular topic in the media. On the basis of this and in partnership with other organisations we successfully argued for a six month pause in the roll out of care.data.

In the main this response covers the proposals for Accredited Safe Havens (ASHs). We also make important points about the nature of the consultation and about information governance standards that should increase patient and public confidence.

Healthwatch England welcomes the Secretary of State's strong commitment to people's right to object to personal data being transferred out of the GP's surgery for research purposes. In September 2013 he said that sharing information securely is a major part of making health services safer. "But if someone has an objection to their information being shared beyond their own care, it will be respected. All they have to do in that case is speak to their GP and their information won't

leave the GP surgery"[1]. This commitment goes significantly beyond the principles in the NHS constitution. Despite the Data Protection Act and the Caldicott Principles this commitment is not yet a legal right to control personal data. We consider that the principle of the Secretary of State's commitment should underpin the broader protection of health and social care personal data. The assurances of the Government (as referenced above), the Partridge Report and the Health and Social Care Information Centre response on care.data should apply to all the information to be collected and disseminated by the proposed ASHs. The right for objection should not be less valid if the information is being collected by an ASH or HSCIC – from a GP or a hospital or another provider.

It is not reasonable to expect patients to understand that their objection to their information being shared will be respected by one part of the NHS but not by another.

Overall key points:

- Safeguarding personal data is an issue that goes beyond the terms of this consultation. It is not clear why this particular consultation does not include care.data. Any new regulations must also synchronise with the data safeguarding clauses in the Care Act, and be built on the principles of the Data Protection Act (and the underlying European Directives) and the Caldicott Principles. There should be a single regulatory framework for personal health and social care data, and a single regulatory body to oversee it. In the absence of a single framework there must be equivalence across the different regulatory frameworks.
- The timeframe proposed for enacting the proposed regulations (before the end of 2014) is unrealistic. We consider that more time needs to be allocated for proper scrutiny.
- We support the setting up of ASHs and sharing of data for clearly defined purposes. ASHs must be subject to a common regulatory framework that applies to all users of personal health and social care data: if that is not possible the framework for ASHs must be equivalence to other information governance systems.
- The consultation paper is not clear whether the accreditation of ASHs is a "one-off" process. To maintain patient and public confidence each ASH should be accredited for a fixed period (3-5 years) with annual audit and review, and a comprehensive reassessment before re-accreditation for another period is possible. Ideally the review period should be shorter in the early phase of implementing the ASH proposals.
- It must be clear that accreditation occurs only for organisation whose purpose justifies the use of patient data and that organisations will lose their ASH status if they fail to comply with information governance standards.
- We have concerns about the proposed structure and plans for how the ASHs will operate and be monitored. For example it is unclear as to whether third party organisations may be able to pay for information held by the ASHs. Also unclear is whether GPs, hospitals and other providers will send information to ASHs on a voluntary basis, or whether they may be paid for it.
- Each ASH should be accredited for a specific purpose, for example research or financial management, rather than all the purposes listed in the consultation. This would enable assessment against purpose and avoid mission creep or aimless data trawling.

[1] https://www.gov.uk/government/news/jeremy-hunt-confirms-commitment-to-balance-patient-safety-and-privacy--2

- Each ASH should have a designated individual to be accountable as information governance risk owner for the ASH (i.e. a Senior Information Officer with relevant experience and qualifications). We are concerned about any potential breaches of confidentiality and the penalties that are set out in the consultation are very light. The Information Commissioner's Office can issue a fine of up to £500K for serious breaches of data protection. We do not understand why the consultation proposes a smaller sanction (£5K) for breaches by the ASHs. This would infer that potential misuse of personal health and care data is not treated as seriously by the Department of Health.
- In the matter of data security we strongly support the 'one strike and out' principle. A serious breach should immediately lead to ASH status being removed.
- In accordance with the Caldicott 2 principle[2]s, (September 2013) and the Data Protection Act, people (patients and social care service users) should have a right to access the information that is held about them and the right to correct information that is incorrect (whether by commission or omission).

Accredited Safe Havens (ASHs)

In addition to answering the specific questions asked in the consultation we are using this opportunity to provider some of our general remarks on the subject of Accredited Safe Havens.

A more harmonised regulatory regime

We generally agree with the basic concept of the Accredited Safe Havens (ASHs), however, we believe that there is a need for a more unified and harmonized regulation on the protection of health and care information.

One goal of the consultation is to: "Establish clear rules on around the use of data that might potentially identify individuals disseminated by Accredited Safe Havens and the Health and Social Care Information Centre". We believe that it would be even more useful to have all personal health and care data uses regulated under a single regulatory regime. That regime should clearly follow the principles of the Data Protection Act and the Caldicott reports.

Paragraph 10 of this consultation suggests that "the care.data initiative is not covered by this consultation but data collected under the care.data initiative could be disseminated to Accredited Safe Havens by the HSCIC, or passed on in accordance with section 4 on controls around broader use of care information". In addition in paragraph 11 specifies that: "a complementary secure data service, the Clinical Practice research datalink, has been established within the Medicines and Healthcare Products Regulatory Agency to service the specialised needs of the research and life communities".

We would like to see more detail of how the proposals will be put into practice so we can be confident that the proposed regulations on Accredited Safe Havens are not being used to bypass the safeguards that the government has promised for the care.data (or vice versa).

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF

Having a single regulatory regime for the collection and dissemination of patient-identifiable data would help to clarify the boundaries of each data collection project and improve the effectiveness and clarity of dissemination of information to the public on this complex issue.

Paragraphs 23 and 24 suggest a weakening of the 2002 regulations and the Care Act 2014 so that an ASH does not have to seek ethical approval or Secretary of State approval for each individual research project. We cannot agree to this unless each ASH is subject to the regulatory regime (regular audit and review, restricted purposes) that we propose. There is no adequate explanation or justification for why the 2002 Regulations (and the more recent 2014 Care Act provisions) should be side-stepped by the ASH system.

Right to object

Concerning the patients' right of objection for the use of their personal data, Paragraph 19 states that "In line with the NHS Constitution, if individuals object to data about them being used in this way, their objection should be respected and their data will not be used".

We believe that this gives a much weaker right to object compared to the guarantee provided by the Secretary of State stating that anyone objecting to the uploading of the GP record to care.data will have that objection honoured. The NHS Constitution says (page 8): "You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis." This right to request is not a right to have this request honoured. Longer term, Healthwatch England wants to explore options for establishing a legal right to object. For the purposes of this consultation, we insist that the ASHs cannot be used to collect and disseminate data about patients who have exercised their right to object under the care.data programme.

Government's assurances on care.data (see footnote 1, page 1) should apply to all the information to be collected and disseminated by ASHs and HSCIC. In addition consumers should have a right to clear information which enables them to choose whether or not to object.

Paragraph 24 of the consultation paper specifies that work on this is being carried out "in parallel with this consultation." We believe that work on this point should be a fundamental part of this consultation rather than being separate.

We want to see more details on how patients can register an objection to their general practice and hospital information being uploaded to an ASH. In particular we require further clarifications on the following points:

- Will the codes that GPs apply to patients' records for care.data purposes apply for ASH purposes?
- How will hospitals, mental health and other providers apply objection codes to patient files, given their variable technologies?
- Are there to be Type 1 and Type 2 objections, as for care.data?[3]

Our response to the specific questions in the consultation is below. We have focused on those most relevant to the role and remit of Healthwatch England.

[3] *Type 1 objection*: Patients can object to information about them leaving a general practice in identifiable form for purposes other than direct care, then confidential information about them will not be shared. *Type 2 objection*: Patients can object to information about them leaving the HSCIC in identifiable form, then confidential information about them will not be sent to anyone by the HSCIC.

Q1. Are these purposes the right ones? Are there any other purposes that it is acceptable for an ASH to use data for? Please set out what you think the purposes should be.

The list of allowable purposes specified in paragraph 26 is wide. Any accreditation of a specific Safe Haven should specify which of the purposes it is allowed to collect and process data for. If an ASH does not use all of the purposes that it is accredited for then its approval should be amended to remove the purpose(s) not used. No ASH should be accredited for all purposes.

Paragraph 20 specifies that "ASHs will be able to obtain data from bodies such as local providers. These local flows will also contain person-level data that is capable of being used to re-identify individuals". We suggest that the HSCIC should be informed about which information ASHs share between themselves.

Paragraph 25 states that: "These new Regulations will not stop any legal data sharing agreements, including those that require data at an individual level between Government departments". While we agree on this principle we believe that the public needs to be informed about how personal data are used between government departments for transparency.

The current consultation does not explicitly define whether GPs, hospitals and other providers will send information to ASHs on a voluntary basis, or whether they may be paid for it. This is a point we believe needs to be clarified.

Q2. Are there any other regulatory controls that you think should be imposed?

The consultation appears to create a "one-off" process for accrediting (or approving) ASHs. This is not acceptable, particularly as the consultation proposes that ASHs will be exempt from the safeguards in the 2002 Regulations and the 2014 Social Care Act. Accreditation should be for a time-limited period (preferably three to five years) with re-accreditation subject to an independent audit of information management (for example to NHS information governance standards and/or ISO/EC 27001:2013(en) standards).

We agree with paragraph 34 where it states that "approval could be removed if the body failed to comply with the controls outlined above, and that the approval will be renewed annually". Re-accreditation should be subject to an independent audit of information management (to NHS information governance standards and/or ISO/EC 27001:2013(en) standards).

In addition paragraph 34 refers to an annual "approval" process though it does not specify the mechanisms that would trigger "disapproval". In particular the failure to provide an independently audited annual statement of compliance with the Information Governance Toolkit (or failure to demonstrate compliance) should trigger temporary or permanent removal of accredited status.

The consultation is far too vague on what happens if an ASH misuses data. We require additional specifications of the possible sanctions to ASHs when they misuse their data. Sanctions should include the possibility of losing accreditation.

If an ASH is required to provide evidence on how it cleans irrelevant data then the evidence should be part of the conditions of accreditation and re-accreditation (and annual approval as in paragraph

34). The evidence should also be subject to a random independent audit (as already provided for later in paragraph 28).

It is important that clear regulations and guidelines on how an ASH will provide data to third parties are in place. All the regulations on data sharing with third parties should be developed in accordance to the Caldicott 2 principles and the Data Protection Act. The data release should be anonymised as much as possible[4]. In addition exchanged data should be encrypted. The exchange agreement should make sure that the data is destroyed once the data agreement period terminates. Audits should ensure that the data has been destroyed in accordance with information management principles.

The second point of paragraph 28 indicates that "an ASH would be acting with the benefit of any guidance on ASH working practices published by the HSCIC or the Secretary of State". This guidance must be produced before the Regulations are enacted and it should be specifically referred to in the Regulations and in the audit and review processes for ASHs.

Paragraph 30 expects ASHs to reduce or eliminate handling of identifiable information. The accreditation process should require a progress report on reduction or elimination, and that ASHs should report each year (as part of the approval/audit) on the steps they have taken towards minimising identifiable data.

Paragraph 18 states that identifiers that are not necessary to the processing will have been removed (for example names and addresses). In addition paragraph 20 states that "Some of the information that ASHs would use could come from HSCIC in the form of standard minimum datasets containing person-level data from which some identifiers have been removed but which is capable of being used to re-identify individuals". Clarity on which identifiers will <u>always</u> be removed when an ASH provides data to third parties could be an important point to communicate to the public to gain trust.

In addition the ASH needs to ensure that it presents the required capacity and technical know-how to ensure that data security is satisfied. Each ASH needs the technical capability to understand that the use made by any third party will not lead to patient identification. Requirements on this should be developed by the HSCIC or by an independent auditor. The technical ability should relate also to all the controls specified in the regulation.

Paragraph 22 makes it clear that ASHs will multiply the number of datasets that contain patient identifiable data to different extents. We need to make sure that security measures are in place when storing the data and when communicating with third parties. This makes it clear that ASHs need to have the technical capabilities and know-how to manage those data. This technical capability could be assured by requiring that the officers of the ASH have a necessary professional qualification in information governance.

ASHs and the HSCIC should control the final information produced from users of patient identifiable data to ensure that the final output does not accidentally lead to patients being identified. This might particularly be the case when performing research on rare diseases or in rural areas. The ASH and the HSCIC should be aware of the final product of research and ensure patient anonymity and confidence is always satisfied. This could be ensured by establishing the figure of a Senior Information Officer in each ASH having the responsibility of the managing of information flows into and out of the organisation.

[4] Information Commissioner's Office Code of Practice - Anonymisation: managing data protection risk (2012)

We request an additional clarification on Paragraph 31. This paragraph states that "as the capacity of the HSCIC increases, we will consider whether the HSCIC is itself a practical alternative to processing within an ASH". Will this imply that in the future the number of ASH will be strongly reduced? Are ASHs needed only until the HSCIC increases its capability?

We would also like to receive additional clarifications what happens to data if an ASH loses or gives up its accreditation.

Q3. What are your views on the maximum amount of the civil penalty that we should set for breach of the controls proposed above in relation to ASHs?

Paragraph 29 proposes a civil penalty for breaches of the guidelines. A better sanction would be temporary (until proof of compliance is produced and independently audited) or permanent withdrawal of a whole organisation's status of ASH.

We are concerned about any potential breaches of confidentiality and the penalties that are set out in the consultation are very light. The Information Commissioner's Office can issue a fine of up to £500K for serious breaches of data protection so why is such a small amount being proposed (£5K) for the ASHs? This would imply that potential misuse of personal health and care data is not treated seriously by the Department of Health.

Equally there is no recompense to an individual or an organisation – say a GP practice – that has been impacted by a breach in confidentiality and from a consumer perspective, this needs more consideration.

Q4. Should there be any restrictions as to the type of body which might become (in whole or in part) an ASH, for example, a social enterprise, a private sector body or a commercial provider (working under a data processor contract)? Please let us know what you think.

Our view is that there should be restrictions on the kind of institution that might become an Accredited Safe Haven. ASHs should only be:

- Organisations In the public sector,
- Charities or Community Interest Companies, and
- Universities and other institutions or Higher Education.

Organisations working in the private sector and serving primarily commercial purposes should not be entitled to become ASHs.

In addition we require that organisations that have acquired, or are interested in acquiring, the status of Accredited Safe Haven will lose that status if they move to the private sector. One example of this latter category would be Commissioning Support Units which are due to start moving into the private sector from 2015. This type of organisational change should trigger an automatic review of accreditation.

No organisation that undertakes activities that raise conflicts of interest should be eligible for ASH accreditation. The sale of personal health and care information to private insurance or medical companies by the forerunners of HSCIC led to serious concerns about care.data. These type of episode severely reduced public confidence in data security.

Paragraph 35 refers to an independent scrutiny of (a) the process for establishing an ASH and (b) the need for these regulations. The regulation should also cover the processes that test / ensure that an organisation is fit to remain an ASH.

The kind of organisation that can gain an ASH status should be restricted to the organisations whose main or only functions are those listed in paragraph 26.

Q5. Is there a maximum number of accredited safe havens that you would consider to be acceptable? Please give your reasons

The number of Accredited Safe Havens should be small, but not too small that it restricts the potential to gain the health and care benefits. Having ASHs with specific parameters and restricted purposes – for example for research or financial transactional analysis - might make a larger number more acceptable.

There is already a national Accredited Safe Haven (the Health and Social Care information Centre) whose powers are determined by statute (the 2012 Act, supplemented re care.data by the Care Act 2014.) In our view it would not be acceptable to set up an indeterminate number of other ASHs, which may operate at national or local level, perhaps in competition with each other, and with no indication of their size. Could an entire CSU be declared an ASH, giving all employees access to information In order to "improve patient services"? We would advise against this scenario.

There are already 56 organisations that are deemed to have met the requirements imposed under section 251 of the NHS Act 2006 to become temporary stage one Accredited Safe Havens, the majority being CCGs or CSUs. Their accreditation will last until October 2014 but it is unclear what the next steps are, how many of these will become ASHs longer term, whether it is assumed these organisations will automatically transfer, or how many more will be set up.

Q6. What are your views on the level of the civil penalty that we should set for providers who do not comply with this duty?

This aspect of the consultation refers to commissioners' access to data from service providers to effectively carry out the commissioning function. We are in favour of the duty. However, the regulations (or guidance) must make it clear that any information request and disclosure is still bound by a duty of confidentiality (extended to the commissioner) and the Data Protection Act. Equally we would like to see 'commissioning purposes' more clearly defined. Are there any limits or at the minimum a list of relevant activities? Information governance principles must still apply to the commissioner and in this respect we would like to see more synergy between different information governance regulations.

As an additional measure to the civil penalty concerning a provider's lack of compliance it could also be an option for the commissioner to recommend to the CQC that the provider's registration be reviewed.

Q7. Do you agree with the circumstances in which commissioners (case managers) should be able to obtain confidential patient information of an individual for whom they commission care?

Paragraph 45 is too general. It does not specify the purpose. Could it be a way to apply section 251 of the National Health Service Act 2006 for any kind of purpose using patient-identifiable data? We would like more clarity in order to understand what this entails.

Whilst the consultation is explicit that this section refers to data beyond the remit of ASHs, paragraph 48 would appear to infer that patient data will be shared and user between service commissioner and provider, despite any individual objection to this use of data and this is unavoidable. What is the value of opting out in this case? More clarity is needed and it is important that people's wishes and choices concerning privacy of personal data are honoured as far as possible. The public need to be clear about any scenarios where their specific wishes in respect of personal data security may potentially be contravened.

Q8. What controls do you think should be in place in respect of such access? Please provide details.

We think that the independent scrutiny (paragraph 48) should be jointly managed by the information commissioner and the CQC. Alternatively, if an independent reviewer (of this and of the ASH proposal) is set up, then we recommend that Healthwatch England is represented on its governing body.

Regarding access control specified under Case Management there should be a requirement that the commissioner and/or the person countersigning the request have an appropriate professional qualification.

After our protests, the Care Act 2014 gave additional assurances about the uses to which HSCIC could put the information collected via care.data (mainly in section 122 of the Care Act.) One of these assurances was that the Health Research Authority's Confidentiality Advisory Group would decide whether any dissemination of potentially identifiable information is appropriate. Why not similar checks over dissemination by an ASH? The Government also promised "one strike and you're out" rule to govern CAG advice – requiring that an applicant requesting data has not misused this sort of data in the past. Why not a similar regime for ASHs? Paragraph 52 of the consultative document mentions CAG in relation to HSCIC, but the subsequent paragraphs don't in relation to ASHs.

Q9. What are your views of the controls set out above?

Again the opportunity to provide a single point for the regulation of data collection, storage and release is lost. Why are the proposed regulations on the role of the confidentiality Advisory group being progressed separately (Paragraph 52)?

The proposed standards in paragraph 57 provide no comfort for those of us concerned about the inappropriate / unethical use of data (paragraph 51)

The proposed penalties only apply to the receivers of information, not the providers (HSCIC or an ASH). This is inequitable. In addition to DPA penalties there should also be provision for suspension,

restriction, or termination of ASH accreditation. Penalties on HSCIC should be extended to enable the Secretary of State to send in someone to sort things out (a breach of this sort should be a 'never event') In addition the civil penalty should be supplemented by administrative sanctions involving temporary or permanent loss of access to HSCIC / ASH data.

We welcome the purpose of providing the existing Confidential Advisory Group (CAG) with an advisory role in respect of disclosures of data by HSCIC, as indicated in paragraph 52. In addition we ask, in line with the recommendations for action following the Partridge review[5], that patients and public representatives will be part of the new membership of the HSCIC data oversight committee, the Data Access Advisory Group (DAAG). It is fundamental that patients and members of the public have a representation in the CAG.

Again an effective penalty on third parties who breach the confidentiality of data is that they might be denied future access to data held by ASHs in the future.

Q10. What are your views on the level of the civil penalty that we should set for any breach of these controls?

In line with our responses on questions 3 and 6 we want to see a system of penalties that is commensurate with the seriousness of the breaches involve, and which complements the powers and sanctions of the Information Commissioner's Office. We do not consider a threshold of £5,000 to be sufficient.

Q11. Are there any other controls that you think should be imposed? If so, please set out what you think these should be.

Paragraph 57 of the consultation document refers. The first point refers to a possible event not likely to be actualised. Can this really be translated into the legal language of regulations? It would be simpler if the HSCIC or ASH placed a requirement on recipients to ensure that:

- They would not come into possession of information that would potentially identify individuals.
- They would not attempt to process information in order to identify individuals.
- They could demonstrate their systems to ensure compliance with the non-possession and non-processing requirements.
- They would open their systems to random audit by ASH / HSCIC (and the Secretary of State's, or the Information Commissioner's investigators).
- They would not release data onwards to third parties without the express permission of the HSCIC or the relevant ASH

[5] "Data release review. Health and Social Care Information Centre. June 2014". http://www.hscic.gov.uk/media/14246/HSCIC-Data-Release-Review-PwC-Final-Report/pdf/HSCIC_Data_Release_Review_PwC_Final_Report.pdf

Q12. Do you think any of the proposals set out in this consultation document could have equality impacts for affected persons who share a protected characteristic, as described above?

More detailed consideration is required in terms of protecting the rights of vulnerable people, particularly those (including children) who do not have capacity to give informed consent. There is nothing in the proposals about them, nor are there any links to other provisions in legislation that might protect them. This needs to be clarified.

Q13. Do you have any views on the proposals in relation to the Secretary of State for Health's duty in relation to reducing health inequalities? If so, please tell us about them.

The Secretary of State's ability to meet the duty will be weakened if there is a loss of public confidence in the handling of personal health and social care data.