Department of Health

Protecting Health and Care Information

A consultation on proposals to introduce new Regulations

June 2014

Title: Protecting Health and Care Information
Author: Information Goverance / Information and Transparency / 13630
Document Purpose: Consultation
Publication Date: June 2014
Target Audience: Department of Health Arm's Length Bodies Providers of healthcare and adult social care Commissioning Organisations Local Authorities The General Public Patient Representative Groups
Contact Details: Jennifer Byrom Quarry House 2N12 0113 254 6102 jennifer.byrom@dh.gsi.gov.uk

Published to gov.uk, in PDF format only.

www.gov.uk/dh

Protecting Health and Care Information

A consultation on proposals to introduce new Regulations

Prepared by Department of Health

Contents

Foreword

Dr Dan Poulter - Parliamentary Under Secretary of State for Health

As a doctor myself, I know that the very best care for patients is delivered when different parts of health and care services work together and a key part of that is about sharing patient information. In an ideal world, all health and care professionals would share all the right information about their patient, in a safe, secure and in a timely fashion so that the person gets good care with no repeating themselves and their histories, no waits while paperwork is passed around, and no mistakes made because one part of the system isn't talking to another.

However, as Dame Fiona Caldicott pointed out in her review, people are concerned about what happens to their information, who has access to it, for what purposes it is used, and why it isn't shared more frequently when common sense tells them it should be. She also pointed out that where information needs to be shared for commissioning purposes, there need to be strong controls around how it is used.

The purposes that information is used for are clearly very important. Whilst most people obviously support information sharing for good quality care, we have heard a lot of concern about individuals' confidential data being provided to insurance companies or other commercial bodies. We intend to make it clear, through regulations, that there must be no abuse of trust and that information collected for important purposes like commissioning or delivering public services will be used appropriately and subject to strong security controls.

With all that in mind, this consultation signals our intention to make some important changes:

Creating new safeguards around information sharing for the purposes of commissioning and understanding population health needs – requiring information to be processed in 'accredited safe havens'.

Establishing clear rules around the use of data that might potentially identify individuals disseminated by accredited safe havens and the Health and Social Care Information Centre.

Clarifying the rules on when information about people receiving health or care services, particularly the most vulnerable, must be shared by those providing the care with those who commission it.

I hope that everyone who has an interest in making sure NHS and care services are run securely will respond to this consultation, so we develop regulations that will help patients and other service users get good, safe, care.

1. Introduction

1. The opportunities and benefits of appropriate data sharing have been acknowledged by all to enable the quality and safety of services to be monitored, measured and improved, but people have to trust that their information is properly safeguarded. Review after review has identified the failure of professionals to share information as a causal factor in child deaths and other tragedies.
2. These proposed Regulations are an important step on a journey to ensure that, for purposes other than direct care:
   - the minimum necessary level of identifiable information is used to support any particular purpose;
   - there is a clear lawful basis for all uses of information; and
   - there are robust controls in place to prevent security breaches or misuse of information.

   As technology develops and information quality improves, the need for staff to access identifiable information will reduce and opportunities for individuals to exercise control over how information about them is used will increase.
3. To achieve this, we envisage that, over the medium term (within, say, three to five years):
   - access to data will be more automated so that routine functions, including many commissioning functions, will not require access to identifiable data itself;
   - the Health and Social Care Information Centre (HSCIC) will be the environment for holding identifiable data at the national level with a number of other smaller safe havens able to access identifiable data for these purposes; and
   - consent will be used more widely as the means to share information.
4. This consultation is carried out under section 251(9) of the National Health Service Act 2006[1]. It sets out proposals for new regulations to place strong controls around the disclosure of data which might potentially identify individuals by the HSCIC and accredited safe havens.
5. This consultation also includes proposals for new regulations to address concerns about restrictions on the sharing of confidential personal information with NHS and social care case managers who need to have access to this information in relation to those for whom they are responsible for arranging health or care services. No serious case review has ever said that 'too much information was shared between organisations' though the opposite has all too frequently been the case. Proposals for establishing accredited safe havens which place strong controls on the sharing and use of data for activities such as commissioning are also outlined.
6. Subject to Parliamentary approval the new regulations are expected to be in place by the end of 2014. They will be informed by the responses to this consultation.

[1] Section 251(9) of the 2006 Act imposes a duty on the Secretary of State, before making regulations under section 251(1) in connection with requiring or regulating the processing of patient information for medical purposes, to consult, to such extent as he considers appropriate in the light of his duty to consult separately with the Care Quality Commission, such bodies appearing to him to represent the interests of those most likely to be affected by the regulations as he considers appropriate.

7. This consultation document sets out in more detail the rationale behind the proposed new regulations. Summaries of previous reviews which have a bearing on these new proposals are provided in Annex B.
8. This document considers separately the regulations relating to the disclosure of potentially identifiable data by the HSCIC and accredited safe havens, those intended to provide controls around broader use of care information and those intended to support vulnerable people receiving care, as the factors to be considered are different in each case.
9. For any data sharing initiative it is important that there is clarity on how the information will be used and by whom, the safeguards around the information and also how and to what extent people will be able to object to their information being part of that specific data sharing initiative.
10. Separate to the proposals in this consultation paper, care.data is an ambitious data sharing project that will bring together information from GPs, hospitals and, over time, other sources to provide the most comprehensive source of care data in the world. It will be an important component of the new data service within HSCIC mentioned in paragraph 3 above. 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 (see section 2), or passed on in accordance with section 4 on controls around broader use of care information.
11. Also separate to the changes proposed in this consultation, more data is already being made available for health and care research in this country, not least through the wealth of data collected, linked and then made available appropriately by the HSCIC. In addition – drawing on data held by the HSCIC and from other sources – a complementary secure data service, the Clinical Practice Research Datalink[2], has been established within the Medicines and Healthcare Products Regulatory Agency to service the specialised needs of the research and life sciences communities.
12. Where a specific research project may need to access more readily identifiable data, The Health Service (Control of Patient Information) Regulations 2002 made under section 251 of the National Health Service Act 2006[3] (referred to in this consultation document as 'the 2002 Regulations') can allow researchers, public health staff and other medical practitioners to access appropriate information where there is no reasonably practicable way of obtaining consent. They are able to use such information for the purposes of medical research that is in the interest of improving patient care or in the public interest.
13. The regulations proposed by this consultation document would apply in relation to England only.

[2] www.cprd.com

[3] http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/

2. Accredited Safe Havens

14. For many years, a statutory basis has been provided, through the 2002 Regulations, for data sharing for a range of essential care services purposes. Examples of the benefits of data sharing include to:
    - find more effective ways of preventing, treating and managing illnesses;
    - make sure that any changes or improvements to services reflect the needs of the local patients;
    - identify who could be at risk of a condition or would benefit from a particular treatment;
    - make sure that NHS organisations receive the correct payments for the services they provide; and
    - guide decisions about how to manage NHS resources so that they can best support the treatment and management of illness for all patients.
15. Sharing information is fundamental to the delivery of modern care services but without a clear statutory basis many organisations would be concerned about the risk of breaching confidentiality law and might be reluctant to share data. The 2002 Regulations have provided a statutory basis for sharing information relating to the health of individuals for certain medical purposes, and each purpose has been considered by the HRA appointed Confidentiality Advisory Group (CAG). CAG provides independent expert advice and each purpose has been agreed by CAG to be necessary, in the public interest and for a care related purpose. On this statutory basis, local commissioners of care are able to access information about individuals in order to identify care needs, analyse care provision and - where the information is confidential patient information - to ensure that the access is lawful, despite the duty of confidentiality which applies to the information.
16. However, whilst this has enabled key activity to be carried out, the existing Regulations do not provide either the coverage that is required or the strong controls that we believe should be in place to protect information. The Information Governance Review (see Annex B) recommended that data sets containing confidential personal data, or data that could potentially identify individuals and that need to be linked for the purposes of population based research, statistical analysis, audit, surveillance and service improvement, should only be brought together in secure environments known as ‘accredited safe havens’ (ASHs). Whilst our proposals differ in some respects from those recommended by the Review, reflecting concerns that many parts of the care system cannot yet work within the precise arrangements it recommended, they seek to deliver similar safeguards.
17. Our vision is that ASHs will provide a secure environment within which data that could potentially identify individuals can be lawfully processed for a limited range of approved purposes, under controls that minimise reliance upon identifiable data and constrain how the data is processed in the ASH. There is more detail about this below.
18. The data that will be used by ASH will be person-level data but as our starting point is that the risk of individuals being identified must be minimised, any identifiers that are not necessary of the processing will have been removed (for example names and addresses). In the wrong hands, the individuals could be re-identified and the controls that we propose

seek to minimise this risk. In line with the Data Protection Act and the Caldicott principles, ASHs will be expected to use only the minimum data necessary for their purposes.

19. In line with the NHS Constitution[4], if individuals object to data about them being used in this way, their objection should be respected and their data will not be used. Work on this is being carried out in parallel with this consultation.

20. Some of the information that ASHs would use would 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. However, those working in ASHs may need access to richer information about individuals than is available from the HSCIC or access to information from providers who do not send data to the HSCIC. Over time, more of this information will be available from the HSCIC but, in the short term, where it is necessary for organisations to have this information, it will come from bodies such as local providers direct to the ASH. These local flows will also contain person-level data that is capable of being used to re-identify individuals.

21. New regulations made under section 251 of the NHS Act 2006 are needed to create ASHs. We propose that these Regulations should limit the purposes for which data can be used and impose statutory controls on the ASHs in addition to providing a statutory basis to share data. The Regulations would enable patient information to be passed from the following bodies to an ASH: the Secretary of State, the HSCIC, NHS England, clinical commissioning groups, local authorities, other ASHs and providers of NHS or publicly funded social care services. The information could be passed for any of the purposes, and would be subject to the controls, which are proposed below. Where the information consists of confidential patient information, the Regulations would enable the information to be passed, despite any obligation of confidence owed in respect of it.

22. Once the ASH has processed the information for one or more of the purposes proposed below, the ASH would be able to retain the information obtained for longitudinal studies i.e. studies which are carried out over a number of years, pass it back to the body which provided it to the ASH and publish it in an effectively anonymised form. Where the information identifies an individual, or could potentially identify an individual, the information could only be disclosed to a third party if there is a lawful basis for that disclosure, which might include disclosure to the patient's direct care team, or if the information is only potentially capable of identifying individuals, in accordance with the restrictions described in section 4 of this document.

23. The 2002 Regulations require bodies who wish to process confidential patient information for the medical purposes described in the Schedule to the Regulations to obtain the approval of the Secretary of State and, in the case of medical research, by a research ethics committee, or following the implementation of the Care Act 2014, the Health Research Authority. We propose that the accreditation of an ASH should require the approval of the Secretary of State but that it would then be permitted to process data for appropriate purposes without further approvals. The ASH would apply for accreditation and the Secretary of State would be advised on the approval by the HSCIC.

24. The provisions in the 2002 Regulations will remain in force and would run in parallel with the proposed ASH arrangements. However, we expect that the volume of non-research activity supported in England through existing approvals under the 2002 Regulations will reduce

[4] www.gov.uk/government/publications/the-nhs-constitution-for-england

over time and be replaced by processing within the ASHs. Authorisations currently in force under the 2002 Regulations would not be affected by these proposals.

25. These new Regulations will not stop any legal data sharing arrangements, including those that require sharing data at an individual level between Government departments.

Purposes

26. The proposed Regulations would set out the broad purposes for which data could be disclosed to an ASH, and for which that data could be used within an ASH. ASHs would be able to link information from more than one source and use it for purposes related to the commissioning and provision of health, public health and social care, but would be limited to the following purposes:

    - making the patient in question less readily identifiable from that information;
    - conducting geographical analysis;
    - analysing differences between population groups;
    - validating and improving the quality or completeness of information, or data derived from such information;
    - auditing, monitoring and analysing the provision made for patient care and treatment, including outcomes, costs and patient satisfaction;
    - understanding and analysing risks to individuals and informing those responsible for their care of the results of that analysis (risk stratification and predictive risk modelling);
    - providing those responsible for providing care to an individual with information that might inform or support that care; and
    - ensuring that the correct payment is made for care provided (invoice validation).

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.

Controls

27. The boundary of the ASH must be clearly established and data only allowed to flow in or out of the ASH and be processed within the ASH in controlled and managed circumstances.

28. It is therefore proposed that the Regulations would also:

    - require an ASH, so far as it is practical to do so, to remove from the data it processes any information which identifies the person to whom it relates which is not required for the purposes for which it is being processed, and to provide evidence of the steps taken towards doing this;
    - take account of the fact 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;

- require an ASH to attribute explicit organisational responsibility for authorising and overseeing information processing and disclosures e.g. to a Senior Information Risk Owner;
- require an ASH not to allow any person access to that information other than a person who, by virtue of his contract of employment or otherwise, is involved in processing the information for an approved purpose – sub-contracting of the processing work would not be permitted;
- require an ASH to ensure that appropriate technical and organisational measures are taken to prevent unauthorised processing of that information and provide evidence of these measures, which we would expect to be by completing and publishing an independently audited assessment of performance annually using the Department of Health Information Governance Toolkit (see Appendix A);
- require ASHs to provide evidence to demonstrate that information that is not intended to identify individuals is not processed with the intention of identifying any individual;
- take account of the fact that any disclosure of personal data (including sensitive personal data) to, and processing of that information by, an ASH would need to comply with the Data Protection Act;
- where confidential information is processed, ASHs will have to make available to the Secretary of State or to the Information Commissioner any information they require to assist in the investigation and audit of that processing;
- require ASHs to review at least annually the need to process confidential patient information and the extent to which it is practicable to reduce the confidential patient information which is being processed;
- require ASHs to publish information on the steps taken to comply with these proposed new Regulations;
- require ASHs to publish a register of data held by the ASH and any information flowing into and out of it;
- require ASHs to report any incidents involving loss of data, information security failing or breach of these Regulations, which we would expect to be through the online incident reporting tool maintained by the HSCIC; and
- allow an ASH only to release data:
    - to third parties directly involved in the care of the data subject,
    - to third parties able to receive the information on some other lawful basis, including in accordance with the provisions described in section 4 of this document; or
    - by way of publication when it has been effectively anonymised, which we would expect to be in accordance with the anonymisation for publication standard published by Secretary of State and NHS England.

29. The 2002 Regulations currently provide for a civil penalty not exceeding £5000 for a person who is in breach of Regulations and we propose that a person in breach of the requirements outlined above should similarly be subject to a civil penalty.
30. Regulations made under section 251 of the National Health Service Act 2006 can only require the processing of confidential patient information where there is no practical

alternative way of achieving the desired aim. In accordance with this principle, we would expect ASHs to implement technology to reduce or eliminate the need for those working in the ASH to handle identifiable information as these become practical options and this check will be made annually as indicated above.

31. At the same time, as the capacity of the HSCIC increases, we will consider whether the HSCIC is itself a practical alternative to processing within an ASH.

32. We believe that these controls on ASHs are at least as strong as those already in place for HSCIC and are stronger than have been in place until now for this type of processing.

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

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?

Who might become an ASH?

33. An ASH would be an existing organisation which is accredited as such by the Secretary of State. It might be an entire organisation or it might be one part of an organisation.

34. We expect that the majority of non-research organisations that are currently processing data under temporary, statutory controls will apply to become an ASH, including commissioning support units and clinical commissioning groups. Bodies seeking to become an ASH will have to be sponsored by the Department of Health or NHS England. The Secretary of State would approve their status as an ASH on the advice of the HSCIC. We propose that the approval could be removed if the body failed to comply with the controls outlined above, and that the approval will be renewed annually.

35. Also annually there will be independent scrutiny of both the process that is followed to establish an ASH and whether these Regulations are still required. We are exploring the options for this independent scrutiny in parallel with this consultation.

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.

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

3. Case Management

36. Commissioners of residential health and care services in England, in exercising their commissioning functions, need to ensure that:-
    - commissioned services deliver high quality and safe care for individual patients;
    - these services are designed to cater for and meet individual needs;
    - wherever commissioning responsibility is transferred between commissioners, patients experience continuity of high quality, safe and appropriate care; and
    - the service commissioned is appropriate and ensures that any risks to the safety of others is minimised and effectively managed.
37. The commissioners of relevant services are Local Authorities, NHS England and clinical commissioning groups. They exercise their commissioning functions when they arrange for the provision of health or social care services. The providers of the services are those who enter into arrangements with the commissioners to provide health or social care services and include NHS trusts, NHS foundation trusts, care homes and other voluntary or private sector organisations.
38. The lessons from Winterbourne View and from the Francis Inquiry (see Annex B) provide a clear understanding that those responsible for commissioning health or social care services must have the ability to monitor the performance of the provider under every contract they commission. In order to do this they need to:
    - have access to quality information generated by the provider;
    - undertake audits, inspections, and investigations; and
    - monitor compliance with standards.
39. Commissioners are sometimes unable to do this effectively for individuals whose care they commission if they cannot access the information contained in care records held by providers in a timely manner, with clear legal authority to do so. This is because a care record is held by a provider under a duty of confidentiality to the individual who is the subject of the record. Whilst confidential information can often lawfully be shared between health and social care professionals who have a legitimate relationship with an individual, the position is more complex for commissioners of health and social care services who are not part of the team providing direct care or treatment.
40. In many cases explicit consent can be sought from the individual receiving care to enable the case manager (i.e. the person or persons within the commissioning body responsible for commissioning that person's care) to obtain the information contained in the care record and it is not intended that best practice in this respect should be undermined by the Regulations. However, there are circumstances where it is not always feasible to obtain explicit consent, or where a person's refusal to the sharing should be overridden. These include:-
    - where it is recognised that there is a potential conflict of interest for providers: to rely on providers to seek consent (or to make decisions in the public interest or determine the best interests of a person receiving health or social care) when there may be quality and safety issues is neither robust nor reliable;
    - where a person receiving care is vulnerable and there are concerns that they may be fearful of those providing them with care and make decisions to please them;

- where an individual is detained in a care setting such as a prison or secure mental health unit they might be reluctant to provide any consent in respect of that care. Nonetheless, arrangements for care still need to be made and tailored to the individual;
- where a case manager needs quickly to obtain details from a range of providers from which it commissions care for an individual to inform a decision about that individual's care, for example in cases when a person with learning disabilities is arrested or committed to a mental health hospital by a court; and
- when an individual is referred to and starts to receive specialised mental health care services or is admitted for treatment under the Mental Health Act, the request for consent may be refused by that individual making it extremely difficult for the case manager to ensure access for the person to the most appropriate care to meet their needs.

41. Through these proposed new Regulations we are seeking to achieve a requirement for providers of residential care to share confidential patient information with case managers, to support case managers to make or monitor commissioning arrangements for the care of vulnerable individuals, where that care includes, or is intended to include, the provision of accommodation. We envisage that the duty to provide the confidential information to a commissioner would apply to a provider who is providing, or has provided, health or social care to an individual, where that health or social care is or was provided by virtue of a contract or other arrangement with the commissioner who is requesting access to that individual's care record. It is envisaged that the duty on the provider to provide the confidential information would also extend to a request from a commissioner who is also, or who subsequently becomes, responsible for commissioning an individual's care (where there may be no contractual relationship with the provider).

42. It is envisaged that a person employed or engaged by the commissioner to commission the health or social care service, or a person who does so on the commissioner's behalf[5] (for example another commissioner in joint commissioning arrangements), would be able to make the request.

43. We are proposing that the Regulations will require a provider to provide the requested information to the commissioner, where the commissioner makes a request to the provider in writing (including electronically). We envisage that the provider will be under a duty to provide the information within the time period stipulated by the commissioner in its written request. If a provider does not comply with the duty, we propose that it would be liable to a civil penalty along the lines of the penalty currently in place in the 2002 Regulations. The 2002 Regulations currently provide for a civil penalty not exceeding £5000 for a person who is in breach of Regulations and we propose that a provider who does not comply with the duty will be liable to such a civil penalty.

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?

[5] For example, this would include a commissioner (A) who acts on behalf of another commissioner (B) to commission care for an individual for whom commissioner B is the responsible commissioner e.g. in respect of out of area placements or joint commissioning arrangements.

44. The commissioners would themselves remain subject to the same duty of confidentiality as health and social care professionals involved in direct care and so would only be able to themselves share the information they obtain under the Regulations if they did so in accordance with the restrictions imposed by the common law duty of confidentiality (and the Data Protection Act). It is envisaged that the Regulations will set out the requirements that a commissioner must meet when requiring information e.g. a clear written record of the concerns held by the commissioner necessitating reliance on the Regulations, the reasons why it would be impracticable to accept an individual's dissent or, where relevant, to seek an individual's consent and the counter signature of a senior manager who works for the commissioner.

45. The Secretary of State can only make regulations under section 251 of the National Health Service Act 2006 requiring the sharing of information for a particular purpose if it is not reasonably practicable to achieve that purpose otherwise than pursuant to regulations, having regard to the cost of and the technology available for achieving the purpose. We do not consider that currently there is any other reasonably practicable way of achieving the proposed purpose, particularly given that an individual's explicit consent to share will be sought whenever it is feasible to do so.

46. The Regulations would ensure that where the information is disclosed by a provider to a commissioner in accordance with the Regulations, it must be taken to be lawfully done despite any obligation of confidence owed in respect of the information. The disclosure (processing) of the requested information must also be done in a manner that is consistent with the provisions of the Data Protection Act 1998[6].

47. These proposals are separate from the accredited safe haven arrangements detailed in the previous section of this consultation.

48. Because of the nature of the proposals it will not be possible for individuals' objections to this use of their information to be respected. Separately to this consultation we are exploring proposals for independent scrutiny and oversight of these arrangements.

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?

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

[6] See section 251(7) of the National Health Service Act 2006.

4. Controlling the Release of Data

49. One of the Government's key aims is to modernise health services and improve health outcomes by putting patients first in every decision that the NHS makes. Underpinning this aim is the need for high quality information so that everybody can make the right decisions at the right time. A modern data service providing NHS organisations, citizens and researchers with accurate, timely information will radically transform the way we care for and treat people and continuously improve the services we offer.

50. As discussed in paragraph 10, care.data will be an important component of this new data service and it is the Government's aim that data sharing to support the NHS, adult social care and integrated care will be encouraged while strictly controlling the use of the same information for purely commercial purposes. To facilitate developments such as this, the Health and Social Care Information Centre (HSCIC) was provided, through the Health and Social Care Act 2012, with powers to collect data from care providers.

51. It has become clear, however, that whilst the majority of people support this ambition, there are significant concerns about the potential for misuse of this information. The Government continues to learn about the public's attitudes towards the use of their data, including through the work done around the introduction of the care.data initiative, and the research into public and professional attitudes towards that initiative is ongoing. In particular it has become clear that many people are unhappy about information being passed – even in a form where the risk of re-identification of individuals is remote – to insurance companies or commercial bodies that might seek to use it for purposes that many would find unacceptable.

52. In response to the concerns mentioned above, we are proposing to put in place a range of safeguards, including to provide the existing Confidentiality Advisory Group[7] (CAG) which provides independent expert advice, to be hosted by the Health Research Authority (HRA), with an advisory role in respect of disclosures of data by HSCIC. Regulations will be able to set out the factors or matters to which the CAG must have regard when giving that advice. These Regulations are being progressed separately and are not the subject of this consultation.

53. Information which does not itself identify individuals could potentially be linked with other information and used to identify individuals by a motivated person. Any dissemination of such data needs to be subject to strong controls to prevent it from being released into the public domain and to prevent any deliberate attempts to identify individuals. We are proposing new regulations to deal with the disclosure by the HSCIC or an ASH of information of this kind (often termed pseudonymised information), that is: information which, whilst not itself identifying individuals, could potentially enable the identity of individuals to be ascertained.

54. Examples of the situations in which we think it would be helpful for this kind of information to be disclosed include medical research, service evaluation, developing models of integrated care, commissioning or delivering other care related public services and understanding population health and public health risks. Evidence from previous reviews reveals that few people would dispute the value of activities such as these but it is essential that information is shared appropriately and is subject to controls to prevent misuse. The proposed Regulations would require HSCIC or an ASH to limit disclosure of potentially identifiable

[7] http://www.hra.nhs.uk/resources/confidentiality-advisory-group/

information made under the Regulations to those who can demonstrate that they are working within the specified controls (see paragraph 57 below). Recognising that it is almost impossible to be 100% certain that any data could not potentially be used to identify individuals, the proposed Regulations would include controls to ensure that recipients of potentially identifiable information are not able to use it to re-identify individuals - thereby giving greater clarity and certainty to HSCIC or to an ASH to assist them in making decisions when and when not to release data.

55. The proposed new Regulations would enable and control the disclosure of this kind of information by setting out clearly what is permitted and what is not. These Regulations would ensure that any breach of the controls would be unlawful, and a civil penalty could be applied. In the 2002 Regulations the current civil penalty is up to £5000.

56. It is also intended that these controls, and any penalty for breach of them, would apply to those who receive this information from the HSCIC or an ASH, to prevent any unauthorised onward disclosure. Our intention is that the recipients of this information would not be processing "personal data" within the meaning of the Data Protection Act because the controls would mean that they would not be able to link it to particular individuals, and nor would they be likely to get hold of information which would enable them to do so. Importantly however, the Data Protection Act will continue to apply and if a recipient engages, in contravention of the Regulations, in processing that results in individuals being identified they would almost certainly be in breach of the first data protection principle in the Data Protection Act (because the processing would be unlawful) which could in some circumstances allow the Information Commissioner to impose a penalty of up to £500,000.

57. We are seeking your views on these proposed new provisions for regulating the disclosure of information that, if misused, could be used to identify an individual. The controls that we envisage applying include:

- preventing HSCIC or an ASH from disclosing potentially identifiable information unless they are satisfied that the proposed recipient is not in possession, and is not likely to come into possession of, information that would enable the recipient to identify the individuals to whom the potentially identifiable information relates;
- preventing HSCIC or an ASH from disclosing potentially identifiable information unless they are satisfied that the proposed recipient is in a position to comply with the controls mentioned below and they have no reason to believe that the proposed recipient has breached the controls when in receipt of this type of information in the past;
- requiring that appropriate organisational and technical measures are taken by recipients to prevent unauthorised processing of information and providing evidence of these measures, which we would expect to be by completing and publishing an annual assessment using the Department of Health Information Governance Toolkit (see annex A);
- requiring that information that is not intended to identify individuals is not processed with a view to identifying any individual;
- imposing a requirement that those in receipt of data must make available to the Secretary of State or to the Information Commissioner such information as they may require to assist in any investigation and audit of the processing that is undertaken;
- preventing any further release of data onwards to third parties without the explicit permission of the HSCIC or the ASH from whom the data came and exactly the same controls being in place to prevent further uncontrolled sharing; and

- requiring that recipients only publish data that is effectively anonymised, which we would expect to be done in accordance with the anonymisation for publication standard[8] published by the Secretary of State and NHS England.

58. We do not propose that disclosures of potentially identifiable information by the HSCIC or an ASH should require the approval of the Secretary of State. Approvals currently in place under regulation 5 of the 2002 Regulations should be unaffected by these proposals. The proposed Regulations would also not affect the sharing of potentially identifiable information which would be lawful when made otherwise than under the Regulations.

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

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

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

[8] http://www.isb.nhs.uk/library/standard/128

5. Equality Issues

59. Section 149 of the Equality Act 2010 establishes the Public Sector Equality Duty (PSED), requiring public authorities to have due regard to the need to:
    - eliminate discrimination, harassment, victimisation and any other conduct prohibited in the 2010 Act;
    - advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; and
    - foster good relations between persons who share a relevant protected characteristic and persons who do not share it.
60. Section 149(7) of the 2010 Act describes relevant protected characteristics for the purpose of the PSED as: age; disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex; and, sexual orientation. It also specifies that Ministers of the Crown and government departments are public authorities for the purpose of the PSED.
61. The Secretary of State for Health has a further duty: he must have regard to the need to reduce inequalities between the people of England with respect to the benefits that may be obtained by them from the health service.
62. The Department of Health's initial view is that there are no potential impacts in relation to the proposed Regulations as regards accredited safe havens and controls on the release of data (sections 2 and 4), as these both impact on care service activity data and are unlikely to impact directly on individuals. The case management aspects of the Regulations (section 3) will, we believe, impact positively on the care of vulnerable individuals for whom accommodation is arranged, some of whom, through age or disability, will belong to the groups protected under the Equality Act, in cases where the care that they are receiving is inadequate or inappropriate.
63. In the development of the new Regulations proposed in this consultation, we must ensure that we have due regard to the three aims of the PSED and the Secretary of State's for Health's duty to have regard to the need to reduce health inequalities. We hope to use this consultation exercise to obtain the views of stakeholders on possible impacts to inform the Department's work to meet its statutory equality duties.[9]

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?

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.

[9] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/276682/2014_services.pdf

6. How to respond

This section outlines the ways in which you can respond to this consultation.

In this document we have set out our aims and intentions to place additional controls on the use and disclosure of information and to clarify the rules on when information about those in care must be shared to support the care of vulnerable individuals. The consultation questions are set out in Sections 2 to 5 above and Annex C.

This consultation is part of the wider engagement on the use and disclosure of information. We have already taken account of previous reports and consultations including the Data Sharing Review and the Information Strategy consultation. We have considered the views on the use of information submitted to the Future Forum and the Information Governance Review, as well as evidence submitted in response to the Francis Inquiry and the Winterbourne View review (see Annex B). We have also taken account of views expressed as part of the engagement exercise on care.data that has been led by NHS England and the findings of their recently concluded consultation on *"Priority Issues in Information Governance*[10]*"* .

It is therefore our intention to consult on the controls on the use and disclosure of information for six weeks, closing on 8 August 2014.

In response to this consultation, you can:

- Answer the questions online at: http://consultations.dh.gov.uk/data-sharing/protecting-health-and-care-information

- Email your response to: **phacd@dh.gsi.gov.uk**

- Post your responses to:

  Data sharing regulations consultation

  c/o Jennifer Byrom

  Room 2N12

  Quarry House

  Quarry Hill

  Leeds

  West Yorkshire

  LS2 7UE

[10] http://www.england.nhs.uk/ourwork/tsd/ig/ig-consultations/ig-priority-issues/

Comments on the consultation process itself

If you have concerns or comments which you would like to make relating specifically to the consultation process itself please contact:

Consultations Coordinator

Department of Health

2e26, Quarry House

Leeds

LS2 7UE

or e-mail : **consultations.co-ordinator@dh.gsi.gov.uk**

Please do not send consultation responses to this address.

Confidentiality of information

We manage the information you provide in response to this consultation in accordance with the Department of Health's **Information Charter**[11]

Information we receive, including personal information, may be published or disclosed in accordance with the access to information regimes (primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

The Department will process your personal data in accordance with the DPA and in most circumstances this will mean that your personal data will not be disclosed to third parties.

[11] http://transparency.dh.gov.uk/dataprotection/information-charter/

Annex A: Information Governance Toolkit Controls

There are approved and comprehensive information governance policies with associated strategies and/or improvement plans
Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations
Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation
Information governance awareness and mandatory training procedures are in place and all staff are appropriately trained
The information governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs
Staff are provided with clear guidance on keeping personal information secure and on respecting the confidentiality of service users
Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected
Individuals (or their parents/carers if appropriate) are informed about the proposed uses of their personal information
There are appropriate confidentiality audit procedures to monitor access to confidential personal information
Where required, protocols governing the routine sharing of personal information have been agreed with other organisations
All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with information governance security accreditation, information quality and confidentiality and data protection requirements
The information governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs
A formal information security risk assessment and management programme for key information assets has been documented, implemented and reviewed
There are documented information security incident / event reporting and management procedures that are accessible to all staff

Monitoring and enforcement processes are in place to ensure NHS national application smartcard users comply with the terms and conditions of use
Operating and application information systems support appropriate access controls and documented and managed access rights are in place for all users of these systems
An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy
All transfers of hardcopy and digital person identifiable and sensitive information have been identified and risk assessed; technical and organisational measures adequately secure these transfers
Business continuity plans are up to date and tested for all critical information assets
Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error
Information assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code
Policy and procedures are in place to ensure that information communication technology networks operate securely
Policy and procedures ensure that mobile computing and teleworking are secure
All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures
The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate

These controls were extracted from the Information Governance toolkit version 11. The controls for version 12, the current version of the toolkit can be found here https://www.igt.hscic.gov.uk/RequirementsList.aspx?tk=64&lnv=4&cb=20%3A41%3A40&sViewOrgType=15

Annex B Previous Reviews

64. There have been a number of reviews that relate to these proposed new regulations. The concept of controlled environments, termed ‘safe havens’ in the 2008 Data Sharing review and ‘accredited safe havens’ in the 2013 Information Governance review, has been debated widely. There seems to be a broad consensus that controlled environments with transparent rules and strong security arrangements in place can provide a secure basis for processing data for purposes other than the direct delivery of care.

65. At the same time, there is a recognition in all the reviews that it is important that information is shared for a wide range of purposes beyond direct care. The stories behind the Francis Inquiry into failings in Mid Staffordshire NHS Foundation Trust and the tragedy of the Winterbourne View hospital clearly call for the barriers to information sharing, whether actual or perceived, to be urgently addressed.

66. Public consultations have consistently found that most people are supportive of information being shared for the right purposes but that there need to be strong controls to prevent it being used for the wrong purposes.

The Data Sharing Review[12]

67. The Data Sharing Review, undertaken by Richard Thomas, the Information Commissioner, and Mark Walport, Director of the Wellcome Trust, considered the use and sharing of personal data in the public and private sectors. The report, published in July 2008, includes a number of recommendations relating to the use and sharing of information for research and statistical analysis. These included:

    “'Safe havens' should be developed as an environment for population-based research and statistical analysis in which the risk of identifying individuals is minimised; and furthermore we recommend that a system of approving or accrediting researchers who meet the relevant criteria to work within those safe havens is established. We think that implementation of this recommendation will require legislation, following the precedent of the Statistics and Registration Service Act 2007.”

68. Although this recommendation was aimed at all parts of government there are particular sensitivities relating to health and social care data. The 2002 Regulations are an existing regulation making power that enable3 the creation of ‘safe havens’ for health and social care data with robust security controls.

The Future Forum[13]

69. The Future Forum report, published in January 2012, set out a number of important principles on the balance between patient confidentiality and the wider sharing of information:

---

[12] http://www.wellcome.ac.uk/About-us/Policy/Spotlight-issues/Personal-information/Data-Sharing-Review/index.htm

[13] http://healthandcare.dh.gov.uk/forum-report

- *Responsible data sharing is an important underpinning of safety, quality and continuity in the care of individuals and, through secondary uses such as clinical audit and research, a vital component of wider learning and quality improvement.*
- *Information governance should be seen as the enabler of responsible sharing and extraction of data in the interests of improving the care of individuals and of wider quality improvements.*
- *It is the patient's and service user's data and needs to be treated with respect.*
- *There should be a normal presumption that all those individuals involved in the care of a patient or service user have access to the data about that person – with their consent.*

70. The report also recommended that an independent review of information governance across health and social care be undertaken, which the Secretary of State for Health subsequently asked Dame Fiona Caldicott to lead (see below).

The Information Strategy[14]

71. "*The Power of Information*" - the information strategy for health and care in England published in May 2012 - set out the Government's proposals for achieving the improvements that are needed in healthcare informatics and information governance. At the heart of these proposals is the requirement to provide:
    - *care records that are effectively shared along the multi-disciplinary, multi-agency individual's care pathway;*
    - *people with greater access to and control of the health and social care information held about them;*
    - *high quality information for secondary uses (R&D, commissioning and planning services, clinical audit and public health).*

Winterbourne View[15]

72. The abuse revealed at Winterbourne View hospital was criminal. Staff whose job was to care for and help people instead routinely mistreated and abused them. Management at the hospital allowed a culture of abuse to flourish. Warning signs were not picked up or acted on by health or local authorities, and concerns raised by a whistle-blower went unheeded. The fact that it took a television documentary to raise the alarm was itself a mark of failings in the system.

73. "*Transforming care: A national response to Winterbourne View Hospital*", published by the Department of Health in December 2012 highlighted a system-wide failure to design, commission and provide services which give people the support they need close to home, and which are in line with well-established standards. Equally, there was a failure to assess the quality of care or outcomes being delivered for the very high cost of places at Winterbourne View and other hospitals.

---

[14] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/213689/dh_134205.pdf

[15] https://www.gov.uk/government/publications/winterbourne-view-hospital-department-of-health-review-and-response

74. As Dame Fiona noted in her report, there are many information governance barriers which are widely seen as preventing commissioners and case managers from accessing the information that they need in order to assess the quality of the care provided to people in need. These proposed new regulations aim to make absolutely clear what information can and cannot be shared for the purposes of commissioning and case management, and by what means.

The Francis Inquiry[16]

75. The Mid Staffordshire review provided a wide range of recommendations on all aspects of care but some were aimed specifically at commissioners, case managers and performance managers. The report published in February 2013 suggests that commissioning as a vital function in the modern health and care system must focus not just on activity and cost efficiency but also on service quality and positive outcomes. The Inquiry's recommendations included:

- *Commissioners must have the capacity and resources to monitor the performance of*
- *every commissioning contract on a continuing basis during the contract period, this may include:*
    - *quality information generated by the provider*
    - *commissioners undertaking their own (or independent) audits, inspections, and investigations*
    - *the possession of accurate, relevant, and useable information*
    - *monitoring compliance both with the fundamental standards and with any enhanced standards adopted.*
- *Commissioners should intervene where substandard or unsafe services are being provided, including requiring the substitution of staff or other measures necessary to protect patients from harm.*
- *Ensuring fundamental patient safety and quality standards are being met and are the top priority for all NHS performance managers. It is essential that "convincing evidence" is provided before assurance is offered.*
- *"Unambiguous lines of referral and information flows" are integral to ensure the performance manager "is not in ignorance of the reality."*

The Information Governance Review[17]

76. The Information Governance Review reported in March 2013 after gathering and assessing an extensive volume of evidence on the balance between data sharing and data security. The Future Forum's key recommendation relating to information governance stated that data sharing is vital for patient safety, quality and integrated care and was endorsed wholeheartedly by the review panel. A particularly important recommendation, providing the basis for elements of these proposed new regulations was that:

    "The linkage of personal confidential data, which requires a legal basis, or data that has been de-identified but still carries a high risk that it could be re-identified with reasonable

[16] http://www.midstaffspublicinquiry.com/

[17] https://www.gov.uk/government/publications/the-information-governance-review

effort, from more than one organisation for any purpose other than direct care should only be done in specialist, well-governed, independently scrutinised and accredited environments called 'accredited safe havens'."

Annex C: Consultation Questions

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.

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

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?

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.

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

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?

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?

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

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

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

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

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?

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.