

Iman Elmehdawy

---

**From:** Jonathan Bamford  
**Sent:** 12 September 2013 12:10  
**To:** Lewis Geraint (NHS ENGLAND) (geraint.lewis@nhs.net)  
**Cc:** Roberts Siobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE) (siobhan.roberts@hscic.gov.uk); Merrett Rachel (NHS ENGLAND); Dawn Monaghan; Steve Wood; David Evans  
**Subject:** ICO comments on awareness raising plans for care.data  
**Attachments:** NHS England letter 12 sept 13.pdf

Dear Dr Lewis,

Please find attached the promised letter in response to your helpful briefing note setting out plans for awareness raising for the care.data programme. I am sending this on behalf of Dawn Monaghan who is out of the office today.

Yours sincerely,

Jonathan Bamford

Jonathan Bamford                      Head of Strategic Liaison

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, United Kingdom.

T. 01625 545752 F. 01625 524510 [www.ico.org.uk](http://www.ico.org.uk)



**Iman Elmehdawy**

---

**From:** Dawn Monaghan  
**Sent:** 19 September 2013 22:44  
**To:** Jacob Smith  
**Subject:** Care.data admin  
**Attachments:** care.data gp practice first wave letter.pdf; 403327.pdf; 403326.pdf; faqs patient care data final.pdf; Response to ICO questions concerning Care Data 26 June 2013.docx; Care Data Data Controllershship.docx

Sorry if you already have this!

D

---

**From:** Thomson Karen (NHS ENGLAND) [<mailto:karen.thomson9@nhs.net>]  
**Sent:** 27 June 2013 16:58  
**To:** Dawn Monaghan; David Evans  
**Cc:** Roberts Slobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Farndon Kathy (NHS ENGLAND); [merrett@bma.org.uk](mailto:merrett@bma.org.uk); Hawkins James (HEALTH AND SOCIAL CARE INFORMATION CENTRE)  
**Subject:** FW: care.data for ICO

Dawn and David

Please find attached our response to the questions you asked. Apologies I have not managed to send this sooner.

Also attached is our analysis of the data controllership and we would be pleased to receive your advice on whether you think this is reasonable.

Also attached are the communications materials which you should have already seen but in case you did not get the final version or have not seen all of them.

I will bring a copy of the draft directions with me tomorrow.

Best wishes

Karen Thomson  
Strategic Information Governance Lead  
Patients and Information Directorate  
NHS England



Queries should be directed to: [England.Information-Governance@nhs.net](mailto:England.Information-Governance@nhs.net)

Admin Assistant: [Redacted]  
[Redacted]@nhs.net

---

**From:** Roberts Slobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE)  
**Sent:** 27 June 2013 16:46  
**To:** Thomson Karen (NHS ENGLAND)  
**Subject:** care.data for ICO

As promised..

Siobhan Roberts  
Programme Manager - Engagement  
Care.data Programme



[siobhan.roberts@nhs.net](mailto:siobhan.roberts@nhs.net)

.....  
.....

This message may contain confidential information. If you are not the intended recipient please inform the sender that you have received the message in error before deleting it. Please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents: to do so is strictly prohibited and may be unlawful.

Thank you for your co-operation.

NHSmail is the secure email and directory service available for all NHS staff in England and Scotland  
NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and GSI recipients  
NHSmail provides an email address for your career in the NHS and can be accessed anywhere

.....  
.....

*Siobhan*

## Data Contollership - Care.Data

The purpose of this paper is to consider the issue of Data Contollership in relation to the Care.Data programme. It covers:

- The definitions of Data Controller and Data Processor
- The available options in relation to data contollership and their feasibility
- Conclusion/Recommendation

### **Data Controller – Definition**

A *Data Controller* is a person who (either by themselves or in conjunction with other people), determine the Purpose for, and the Manner in which, Personal Data is to be processed.

### **Data Processor - Definition**

A *Data Processor* is a person or persons (not employed by the Data Controller) who process the data on behalf of, or under instruction from, the Data Controller.

### **Care.Data programme**

There are four Data Controller options. Consideration of each is set out below:

Option	Data Controller
1	NHS England as Data Controller, HSCIC as Data Processor
2	HSCIC as Data Controller
3	NHS England and HSCIC as Data Controllers in Common
4	NHS England and HSCIC as joint Data Controllers

### **Option 1 – NHS England as sole Data Controller, HSCIC as Data Processor**

For NHS England to be sole data controller for the Care.Data data collection, it would need the vires to collect this data either through statute or with the consent of the individuals concerned. As NHS England was not given such powers under the Health and Social Care Act 2012, in contrast to the HSCIC, it could only become sole data controller if it obtained the consent of every individual to collect and process their data. As seeking consent from every individual in the country is not practicable, this option is not feasible. The only way this option would be feasible is if NHS England were to obtain support under the Health Service (Control of patient information) regulations 2002 (or new statutory support) but it would need to consider whether other options were feasible.

### **Option 2 – HSCIC as sole Data Controller**

Under the Health and Social Care Act 2012, the HSCIC is empowered to collect confidential information where it is directed or requested to do so, subject to a number of restrictions. As the care.data is an NHS England-led project however, and as NHS England would therefore control the purpose, and (broadly) the manner, it is questionable whether the HSCIC could truly be sole data controller for this programme of work. Even if feasible, this option would mean less direct control for NHS England, although the Directions could be specific, and therefore this is unlikely to be an acceptable option for NHS England.

### **Option 3 – NHS England and HSCIC as Data Controllers in Common**

Under this option both NHS England and the HSCIC would be separately responsible for processing the data for their own purposes. This option is not feasible for the same reasons that option 1 is not feasible – that NHS England does not have the vires to collect and process confidential information itself.

### **Option 4 – NHS England and HSCIC as Joint Data Controllers**

With this option, NHS England would control the purpose and broadly the manner of processing but HSCIC would control the manner more directly and take responsibility for the organisational and technical measures to protect the data. Both parties would share legal liability for the processing of data, including responsibility to inform data subjects of the processing purposes.

This option is feasible because:

- Confidential data could be lawfully obtained by the HSCIC using their powers under the 2012 Act to collect and process confidential information under directions from NHS England.
- This would not give NHS England authority to access the data in identifiable form but NHS England would still be controlling the purposes and broadly the manner of processing through the Directions issued.

### **Recommendation**

Options 1 and 3 are not feasible and whilst option 2 may be feasible it is unlikely to be acceptable to NHS England. Therefore option 4 is recommended as it provides:

- the best fit with the Data Protection Act, and
- retains primary control of the care.data programme within NHS England.

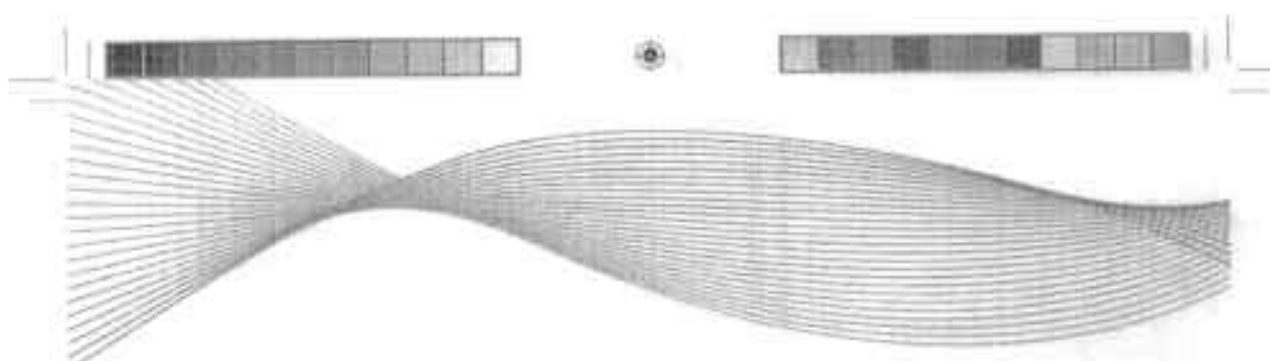
As joint Data Controllers, a memorandum of understanding or agreement is needed setting out the division of data controller responsibilities between the two organisations. All public communications about the programme, also need to be jointly owned and branded (therefore jointly approved) by both parties.



How information  
**about you** helps  
us to **provide**  
**better care**

**hscic**

Health & Social Care  
Information Centre



## Introduction

In some circumstances, healthcare staff share information about your treatment and care to help us to improve the services we offer and the care we provide to everyone. The type of information shared, and how it is shared, is controlled by law and strict confidentiality rules.

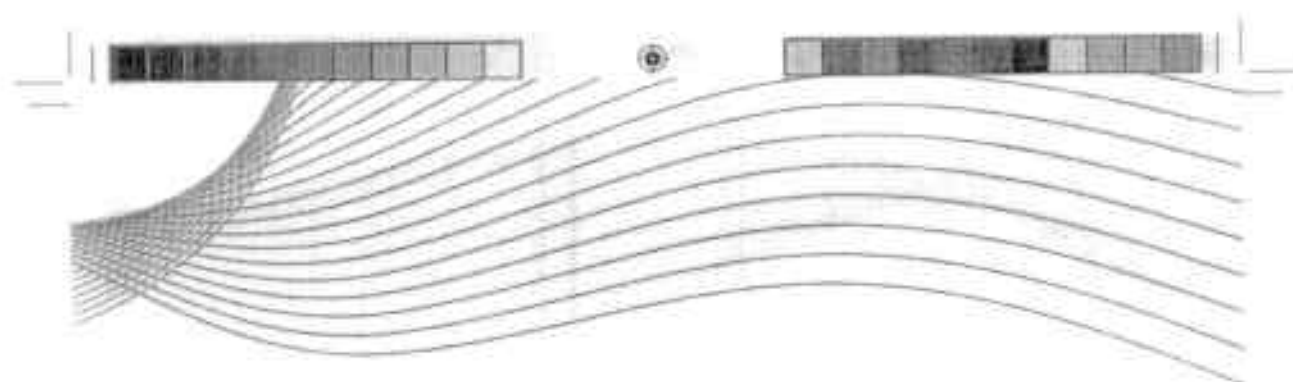
In order to plan and improve care for all patients it is important that we link information from the different places where you receive care to help us provide a full picture. This will let us compare the care received in one area to the care received in another, so we can see what worked best.

Your postcode or NHS number, rather than your name, will be used to link your records in a secure system, so your identity is protected. Information which does not reveal your identity can then be used by others, such as researchers and those planning services, to make sure we provide the best care possible for everyone.

We need to make sure that you know this is happening and the choices you have.

**Please read this leaflet carefully.**





## Benefits of sharing information

Sharing information can help improve understanding, locally and nationally, of the most important health needs and the quality of the treatment and care provided by local health services. It may also help researchers by supporting studies that identify patterns in diseases, responses to different treatments and potential solutions.

Information will also help to:

- find more effective ways of preventing, treating and managing illnesses;
- guide local decisions about changes that are needed to respond to the needs of local patients;
- support public health by anticipating risks of particular diseases and conditions, and help us to take action to prevent problems;
- improve the public's understanding of the outcomes of care, giving them confidence in health and care services; and
- guide decisions about how to manage NHS resources so that they can best support the treatment and management of illness for the benefit of patients.

## What will we do with the information?

We will only ask for the minimum amount of information we need to help us improve patient care and the services we provide.

We have developed a thorough process that must be followed before any information can be shared. We are very careful with the information and follow strict rules about how it is stored and used.

We will make sure that the way we use information is in line with the law and meets the NHS confidentiality code of practice, the NHS Constitution and other national guidance and best practice.

Reports that we publish will never identify a particular person.



## Do I have a choice?

Yes. If you do not want information that identifies you from being shared outside your GP practice, tell your practice to make a note of this in your medical record. This will prevent your confidential information being used other than where necessary by law (for example, if there is a public health emergency).

You will also be able to restrict the use of information held by other places you receive care from.

This will not affect the care you receive.

## Do I need to do anything?

If you are happy for your information to be shared to help improve services, you do not need to do anything. There is no form to fill in and nothing to sign, and you can change your mind at any time.

If you have concerns, speak to your GP practice.

## Will anyone contact me?

We sometimes release information to approved researchers where this is allowed under strict conditions. For most research, patients do not need to be contacted, but in some cases they do. If a researcher needs to contact you, they will only do this with the approval of your own doctor, who will contact you for your permission.

## Where can I get more information?

You can speak to staff at your GP practice.

If you need this information in Braille, easy-read, large print or a different language, please contact us.



## Response to ICO Questions for NHSE and HSCIC

1.	Are we correct in thinking that the legally NHSE should still be referred to as NHS Commissioning Board and that NHS England is a brand not a legal entity?
	Yes, NHS England is a brand. It is the operating name for the NHS Commissioning Board as defined and established under the Health and Social Care Act 2012.
2.	What is the proposed timescale for implementation of the early adopters?
	The early implementers received information on the 12 June and have been asked to display patient information in their practices. After a period of approximately 8 weeks data will be extracted. If, after extraction, those who had not had an opportunity to object at the time wish to do so, then their data can be retrospectively deleted from the care.data data collection.
3.	What is the proposed timescale of National rollout/ will it be phased?
	Following initial feedback collected over the first 4 weeks from the early implementers, supporting information and materials for practices and patients will be reviewed and revised before national roll out begins. Information will be sent to all practices in England via a phased approach over a 2 week period. In terms of timing this will happen before any data is extracted from the early implementers.
4.	Have NHSE given 'formal' direction to HSCIC to collect and process the data if so would it be possible for us to have a copy of those directions?
	Directions are in the process of being drafted in consultation with the Department of Health and the Health and Social Care Information Centre. We would be happy to share the draft directions with you in confidence, and therefore on the basis of being exempt under Section 41 from disclosure under FOIA. Our rationale for not wanting the draft directions to be disclosed is that it would prejudice the effective conduct of public affairs by preventing or inhibiting the free and frank exchange of views for the purposes of deliberation under Section 36(2)(b). Additionally, we intend to publish the finalised directions once agreed and formally approved by all parties and therefore would also be exempt under Section 22.
5.	How will HSCIC 'require' the information from general practices will that be a 'formal' notification if this is the case what will it look like?
	The communication to GP practices is attached.
6.	Do you consider HSCIC to be a Data Processor for NHSE a data controller or both and what is your reasoning for this?
	See attached briefing on data controllership. We would welcome the ICO's

	views on this and confirmation that these arrangements are satisfactory.
7.	Will the HSCIC be informing citizens of who they are what they do with the data etc or will this be part of the communication provided by NHSE?
	The communications for citizens will be jointly badged in line with data controller arrangements i.e. both NHS E and HSCIC.
8.	Are the HSCIC going to use/share the data collected under direction from NHSE for any other purposes than those described in the specified direction?
	It is anticipated that most purposes would be covered under the directions we are in the process of developing. However where purposes fall outside the Directions, these further uses will only happen with the agreement of NHS England, in line with joint data controller arrangements and in relation to data extracted via GPES would also need to be approved by the HSCIC's Independent Advisory Group.
9.	Who is going to complete the PIA for care.data will that be NHSE or HSCIC?
	The HSCIC is in the process of completing a PIA which will include care.data. If the ICO consider that it is necessary for NHS England to conduct a separate PIA please advise us and we will undertake separate to this.





## How information about you helps us provide better care

### Frequently asked questions for patients

#### 1. Why do I need to read the leaflet 'how information about you helps us provide better care'?

It is important that you read the leaflet so that you understand how information in medical records can be used to improve the way that health care is delivered; the services offered by the NHS and for carrying out research into the treatments offered for different diseases and illnesses.

If you are happy for your information to be used then you do not need to do anything but it is important that you know this is happening and what to do if you have any questions or concerns (See FAQ 13).

#### 2. How is information collected?

Information is collected through a new modern information system being developed by the NHS in England. You may have heard this system referred to as care.data. Care.data is the programme name for the new system.

One of the main aims of the new system is to allow the NHS to make better use of the routine information collected when you visit your doctor. The system complies with strict confidentiality rules and the law.

This service will provide joined-up information about the care received from all of the different parts of the health service, including hospitals and GP practices.

It is important that the people who plan and manage health services have access to a full picture of care being provided to patients so that they can make sure that the NHS is providing the best possible services to all of its patients. It can do this by using the information to compare the care received in one area to the care received in another to see what worked best.

#### 3. Who is delivering the system?

The Health and Social Care Information Centre (HSCIC) is working with NHS England to deliver the system on behalf of the entire NHS (see FAQ 6).

#### 4. Why are these changes needed?

It is important we have a complete picture of what is happening across the health and social care service. This will allow those who plan services to see what is working best.

To give you an example: A group of patients could have the same operation but

*High quality care for all, now and for future generations*



receive different aftercare. Those planning and designing health services can look at which aftercare worked best so that all patients can benefit from those experiences. They do not need to have information that identifies you but will need the HSCIC to link the data as described in FAQ 7.

These changes will deliver an effective system for collecting, analysing and sharing data while protecting patients' privacy and confidentiality.

The system will also provide information that will enable the public to hold the NHS to account and ensure that any unacceptable standards of care are identified as quickly as possible.

#### **5. When will these changes occur?**

The new system will begin with a small group of GP practices in the first instance. Your practice may not be one of the first but will make information available to you when they are ready.

The first use of the system will be to help commissioners plan local health services by using linked data which does not identify any person or individual.

A patient leaflet and poster will be tested in GP practices to ensure the messages are clear. The system will then be rolled out more widely over the summer and into the autumn.

Information from GP records will be sent to the secure environment of the HSCIC from August starting with the small group of practices first.

#### **6. What is the secure environment mentioned in the leaflet?**

The secure environment is called the Health and Social Care Information Centre (HSCIC). This is a public body based in Leeds. The HSCIC is the central source of health and social care information in England. The role of the HSCIC is to ensure that high quality data is used appropriately to improve patient care. The HSCIC has legal powers to collect and analyse data from all providers of NHS care.

The HSCIC is committed, and legally bound, to the very highest standards of privacy and confidentiality to ensure that your confidential information is protected at all times. Access to information is strictly controlled. Further information about the HSCIC is available [here](#).

#### **7. Will the people in the secure environment see information that identifies me?**

When information leaves your GP practice, it will be sent to the HSCIC (see FAQ 6). The system at the HSCIC will link information from your GP record with information from your hospital record, if you have one, to create a new linked record. The process to create the linked record will be an automated process which also replaces any information that directly identifies you such as your nhs number, address or date of birth with a code that does not reveal who you are.



Only the linked data record will be used by those planning health services.

Separate to this there are limited circumstances when the law allows the HSCIC to pass on information which may identify you where there is special approval (see FAQ 8). You can object to this (see FAQ 14).

#### **8. What research will be carried out on data that identifies me?**

In most cases researchers can carry out their studies using information that does not identify you. Occasionally, medical researchers need to use information that identifies you. Only researchers who have been granted special approval by an independent panel called the Confidentiality Advisory Group are allowed access to your identifiable information. This group grants approval to a small number of research projects, which it considers to be in the public interest and for the benefit of the health service. Approval is only given if it is not possible to use information which does not identify you and it is not possible to ask you for example, if it involves a large number of patients. Access is also restricted to the specific information necessary for the research.

Examples of projects approved by the group include a national study into people who have had a heart attack and a study of the time people have to wait for treatment for cancer and the effect of these waiting times on survival. More examples can be found [here](#).

#### **9. Will information that identifies me be used by marketing or drug companies?**

Marketing and drug companies will not have access to information that identifies you unless you give your permission, such as if you have been contacted by your GP practice and agreed that researchers could contact you about a clinical trial.

There are some limited circumstances when the NHS needs to carry out medical research using information that identifies you. This requires special approval (see FAQ 8). You will not be contacted by a third party unless you have agreed to this.

#### **10. Will you sell data?**

No. The HSCIC does not charge researchers for data. Sometimes, the HSCIC may charge an administrative fee (for example, to link the data) but there is no commercial sale of NHS data.

#### **11. What data will be extracted - will my whole GP record be used?**

No. Only the minimum amount of information required will be used. Your date of birth, full post code, NHS number and gender rather than your name will be used to link your records in a secure environment before being deleted. Once this information has been linked a new record will be created (see FAQ 7). This new record will not contain information that identifies you.

When your GP enters information into a health record a combination of free text and codes are used. Free text might be something you tell your doctor such as your symptoms, your occupation, how you are feeling. Codes are a combination of letters and numbers that indicate a particular condition. Your GP can search codes using a computer to find all the patients in the practice with the same code and invite those patients to a specialist clinic for that condition. You can see a list of the types of codes that will be used for care data [here](#). The list includes codes about NHS prescriptions, referrals and other clinical information.

Free text information will not be sent to the HSCIC secure environment. Information extracted will be coded information, together with your NHS number, postcode, date of birth and gender. Note that your name and full address will be removed from this extract so your identity is protected.

## **12. Why do you need to extract data that identifies me?**

We need to be able to link information from the different places where you receive care such as your GP and hospital. The people who plan and monitor the quality of NHS services need this type of joined-up information to get a full picture of the care being provided by the health service. Your NHS number, postcode, gender and date of birth are required by the system in the secure environment so that we can join up this information from the different places where you receive care (see FAQ 7). Your name is not used.

## **13. What should I do if I have concerns?**

If you have concerns you can talk to staff at your GP practice or ask the practice for a copy of the leaflet 'How information about you helps us to provide better care'.

If you do not want information that identifies you from being shared outside your GP practice, you can ask your practice to make a note of this in your medical record. This is called an objection. This will prevent your confidential information being used other than where there are exceptional circumstances or where the law allows your information to be shared.

If you are happy for your information to be used for planning health services and for research then you do not need to do anything.

## **14. What kinds of information sharing can I object to?**

There are two types of information sharing you can object to:-

- You can object to information containing data that identifies you from leaving the GP practice. This type of objection will prevent the information held in your GP record from being sent to the HSCIC secure environment and also by those who have gained special approval to use health information for research.

- You can also object to any information containing data that identifies you from leaving the HSCIC secure environment. This includes information from all places you receive care such as hospitals.

**15. If I object will this stop all data leaving the practice?**

No. The law requires doctors to provide some very limited information about certain things. The law says, for example that doctors must provide information to local authorities about some infectious diseases, such as if you had food poisoning. Very rarely, doctors may also be required to disclose information in order to detect a serious crime. A court order can also require doctors to disclose certain information such as during a court case.

**16. I have opted out of the Summary Care Record (SCR) do I need to talk to my GP if I have any concerns?**

Yes, you should still talk to your GP. There are important differences between allowing the NHS to use your information for planning and research and the Summary Care Record (SCR). The SCR is used by health professionals to provide you with care. It would be wrong for us to assume that because you have chosen not to have a SCR that this means you also wish to stop the use of your information being used to improve health services.

**17. Can I stop data being used from other places where I receive care for example a hospital?**

No. Currently, and only where the law allows it, some information will flow from hospitals and other places where you receive care and treatment to the HSCIC. You can only currently object to data containing information that identifies you leaving your GP practice.

However, you can object to any information containing data that identifies you from leaving the HSCIC secure environment. This includes information from all places you receive care for example hospitals.

In the future, it should be possible for you to stop information containing information that identifies you going to the HSCIC from wherever you receive care or treatment. The systems we use in the NHS do not currently allow this so the note of your objection in your GP record cannot be seen by other places you receive care such as hospitals.

**18. Can I stop data that does not identify me being used?**

No. Information that does not identify you is not confidential. Since this information is neither personal nor private the law says that it can be used much more freely. As this information can be very helpful to the NHS and does not identify you, there are good reasons for making the best possible use of it.

**19. Can I change my mind?**

*High quality care for all, now and for future generations*

Yes, you can change your mind at any time and as many times as you wish. For example, if you object and then change your mind and decide you are happy for your information to be used then you will need to speak to your GP practice to ensure this happens. And if you do not object now but then later decide you wish to object this is also possible. Just speak to your GP practice and ask them to record your wishes.

**20. Can I change my mind and decide I no longer want information that identifies me to be used even if it has already gone to the HSCIC?**

Yes. You should notify your GP of your objection. The HSCIC will then ensure that any information they have which identifies you is removed. Alternatively you can contact the HSCIC yourself and let them know you have changed your mind. Contact information for the HSCIC is available [here](#).

**21. Can I have a greater number of choices and allow data to be used for some but not other research projects?**

No. Currently you have the right to say yes or no to your information being used for research but the system does not let you say yes or no to your information being used for all the different types of research projects.

**22. Do I need to do anything if I am happy for my information to be used?**

No. If you are happy for your information to be shared to help improve health services, you do not need to do anything. Your information will continue to be used for that purpose and to benefit all patients.

**23. What happens if my confidentiality is breached?**

The HSCIC is committed, and legally bound, to the very highest standards of privacy and confidentiality to ensure that confidential information is protected at all times. Information in health records can only be shared beyond those caring for you where: (i) the law allows it (ii) there is a court order (iii) there is a public interest or (iv) you have given permission (See FAQ 16).

The [Information Commissioner's Office](#) has powers to impose heavy fines in the event of any breach of the Data Protection Act 1998 (the law which governs how your information is used by organisations, businesses and the government). It also sets out clear guidance in relation to whether data identifies you or not. This is available [here](#).

Dear Practice Manager

## Early implementers of care.data

I am writing to inform you that your practice has been selected as one of the first in England to begin the extract of GP data into the new *care.data* system (<http://www.england.nhs.uk/ourwork/tsd/data-info/>).

This letter outlines what you now need to do, including how to access the supporting materials that we have developed jointly with the British Medical Association (BMA) and the Royal College of General Practitioners (RCGP).

Our guidance is designed to help you:

- understand the purpose of the *care.data* service, including a joint statement from NHS England, the BMA, and the RCGP;
- raise awareness with patients about how their confidential data will be used by the *care.data* service;
- meet your Data Protection *fair processing* requirements;
- understand what to do if a patient objects to the extraction of their confidential data.

### Guidance and Resources

In the next few days, you will receive supporting materials in the post. You can also access these resources online here: <http://www.england.nhs.uk/ourwork/tsd/data-info/>

### What practices need to do now

It is important to ensure that patients are made aware of this new data extract before it begins, and what they should do if they have any concerns or objections:

#### Next steps:

1. Please display the posters in the practice without delay and make the patient information leaflets available to your patients.
2. Please make the same information available on your website and in any routine patient communications, such as e-bulletins and patient newsletters.
3. Please advise your staff that they should respond to any queries or concerns from patients by directing them to the patient leaflet and to our FAQs.

In approximately 8 weeks time, which is the minimum period required to make your patients aware, the Health and Social Care Information Centre (HSCIC) will begin extracting data via the GP Extraction Service (GPES) for those patients who have not objected.

### Your help please

Because you are one of the first practices to participate in the new care.data service, we would be grateful to hear about any comments or feedback you receive from your patients and staff on both the patient materials and guidance supplied. We will use your feedback to help improve our communications.

Please send your feedback to: [enquiries@hscic.gov.uk](mailto:enquiries@hscic.gov.uk) quoting: 'care.data - communications feedback' in the subject line.

### Questions

If you have any questions about the care.data extract, please telephone the HSCIC Contact Centre on 0845 300 6016 (open from 9 am to 5 pm Monday to Friday) or send an email to: [enquiries@hscic.gov.uk](mailto:enquiries@hscic.gov.uk) (quoting 'care.data - GP' in the subject line). Please note that the contact centre can only deal with queries from clinicians and GP practice staff: patient enquiries should instead be addressed by GP practices using the FAQs provided.

Guidance on confidentiality from the GMC is clear that doctors must disclose information to satisfy a statutory requirement. As the Health and Social Care Act (HSCA) creates a statutory obligation to disclose Personal Confidential Data (PCD), GPs will not be in breach of GMC guidance in this case, provided the wishes of patients to object are respected.

We look forward to working with you to support the new care.data service. I am confident that care.data will rapidly be seen as an invaluable resource for clinicians, commissioners, and researchers as we work to improve the quality, efficiency, and equity of the NHS.

Yours faithfully,



**Dr. Geraint Lewis FRCP FFPH**  
Chief Data Officer  
NHS England

**Dr. Mark Davies BSc FRCP FRCGP**  
Director, Clinical and Public Assurance  
Health & Social Care Information Centre



**Iman Elmehdawy**

---

**From:** Dawn Monaghan  
**Sent:** 19 September 2013 16:00  
**To:** Jacob Smith  
**Subject:** Care.data admin

**Importance:** High

Another e mail trail

---

**From:** Dawn Monaghan  
**Sent:** 03 September 2013 10:21  
**To:** 'Merrett Rachel (NHS ENGLAND)'  
**Cc:** Roberts Slobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE)  
**Subject:** RE: Care.data national roll out  
**Importance:** High

Hi Rachel



You are correct about the workload I am drowning in communication. However as always Care.data is high up our agenda and a catch up call this week would be welcome, would 14.00 on Thursday be any good?

Regards  
Dawn

---

**From:** Merrett Rachel (NHS ENGLAND) [<mailto:r.merrett@nhs.net>]  
**Sent:** 02 September 2013 16:35  
**To:** Dawn Monaghan  
**Cc:** Roberts Slobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE)  
**Subject:** FW: Care.data national roll out

Hi Dawn

Welcome back from your holiday! I'm sure you have come back to a huge amount but would it be possible to schedule a call with you this week (except Friday as I'm on leave). We have various things to update you on and it would be helpful to catch up on things from your perspective.

Thanks  
Rachel



**From:** Jonathan Bamford [<mailto:Jonathan.Bamford@ico.gsi.gov.uk>]  
**Sent:** 30 August 2013 08:32  
**To:** Merrett Rachel (NHS ENGLAND); Roberts Slobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Dawn Monaghan; David Evans  
**Cc:** David Smith; Christopher Graham; Lewis Geraint (NHS ENGLAND); Outram Christine (NHS ENGLAND)  
**Subject:** RE: Care.data national roll out

Rachel,

Thank you for the clarification. This is helpful. Dawn Monaghan is back from leave next week so she should revert to being your primary contact at the ICO on this issue from Monday though I will still retain an interest in the issue so please continue to copy me in. Please ensure Dawn and David Evans are sent the information about patient awareness when this is produced.

Thank you for your help.

Regards,

Jonathan

**Jonathan Bamford**                      **Head of Strategic Liaison**

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, United Kingdom.  
T: 01625 545752 F: 01625 524510 [www.ico.org.uk](http://www.ico.org.uk)

---

**From:** Merrett Rachel (NHS ENGLAND) [<mailto:r.merrett@nhs.net>]  
**Sent:** 29 August 2013 18:37  
**To:** Jonathan Bamford; Roberts Siobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Dawn Monaghan; David Evans  
**Cc:** David Smith; Christopher Graham; Lewis Geraint (NHS ENGLAND); Outram Christine (NHS ENGLAND)  
**Subject:** RE: Care.data national roll out

Dear Jonathan

Yes that is correct. We involved your team in looking at the wording of the guidance and FAQs, which refer to making information available. We changed the wording in the final version of the FAQs to specifically mention (as quoted in my previous email) sending information out with repeat prescriptions etc. – this was based on feedback from the pilot GP practices who gave examples of the communication channels they had used.

In relation to your second point, I have liaised again with the HSCIC team and confirmed that these are the main circumstances when data would be extracted without a patient visiting the practice. It is limited to when a GP receives information about a patient's care and enters it into the GP record AND that information fits within the care.data published dataset.

I hope this is helpful.

Kind regards  
Rachel

---

**From:** Jonathan Bamford [<mailto:Jonathan.Bamford@ico.gsi.gov.uk>]  
**Sent:** 28 August 2013 17:05  
**To:** Merrett Rachel (NHS ENGLAND); Roberts Siobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Dawn Monaghan; David Evans  
**Cc:** David Smith; Christopher Graham; Lewis Geraint (NHS ENGLAND); Outram Christine (NHS ENGLAND)  
**Subject:** RE: Care.data national roll out



## Iman Elmehdawy

---

**From:** Dawn Monaghan  
**Sent:** 19 September 2013 16:05  
**To:** Jakob Smith  
**Subject:** Care data admin

**Importance:** High

more

---

**From:** Dawn Monaghan  
**Sent:** 06 September 2013 15:58  
**To:** 'r.merrett@nhs.net'; Roberts Siobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE) ([siobhan.roberts@hscic.gov.uk](mailto:siobhan.roberts@hscic.gov.uk))  
**Cc:** Jonathan Bamford; David Evans; Steve Wood  
**Subject:** Clarification  
**Importance:** High

Hi  
Sorry I know you have had extensive e mail exchanges with Jonathan (which I did had sight of and re read this afternoon) but could you clarify for me the following couple of things.

Firstly;  
The documentation given to GP's to fulfil the communication to Citizens does not appear to actually prescribe to General Practices how they should provide the leaflets/information to individuals visiting the surgery. It only suggests in the check list that you ensure you have received the information materials, displayed the posters and made the leaflets accessible (that could surely just be a pile on a table or a box on the floor) Is that correct or have they/will they be told that each patient on visiting the surgery must be given with a leaflet? Presumably by the receptionist or practitioner (GP/Practice nurse/midwife etc.)

Also;  
In relation to the actual data extraction. Negating whether the extraction is for data anytime post April 1<sup>st</sup> 2013 or some data which is pre April 1<sup>st</sup> 2013.  
Is the intention to only extract data from an individual's record once they make a visit to the GP surgery after the 'Go live' date for initially the early implementers and then national roll out.  
I know you have communicated there are circumstances when data may be extracted when a patient hasn't visited a surgery but I'm not sure we mean the same things. In these instances is this when the data is input from someone other than the surgery rather than an extraction of the data only beginning for that patient once they have visited a surgery.

To help explain if the national rollout goes live on say the 1st Jan 2014 if I don't actually visit my GP until Sept 2016 none of my data will be extracted even if I have not used the objection process and when I do visit my surgery I will be given the patient information leaflet?

Not sure I'm making this very clear so if necessary please call me and I'll try to explain what I mean.

Regards  
Dawn

01625 524510

**Dawn Monaghan      Group Manager, Public Services**

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.  
T. 01625545719 F. 01625 524510 [www.ico.org.uk](http://www.ico.org.uk)

**Iman Elmehdawy**

---

**From:** Dawn Monaghan  
**Sent:** 19 September 2013 22:51  
**To:** Jacob Smith  
**Subject:** Care data admin  
**Attachments:** NHSE Care dataPIAv05.docx; ATT00001.htm

---

**From:** Merrett Rachel (NHS ENGLAND) [mailto:r.merrett@nhs.net]  
**Sent:** 18 September 2013 22:51  
**To:** [REDACTED] (NHS ENGLAND)  
**CC:** Flynn Peter (NHS ENGLAND); Thomson Karen (NHS ENGLAND); Roberts Siobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Dawn Monaghan; David Evans; sanderson clare (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Outram Christine (NHS ENGLAND)  
**Subject:** Re: NHS England and ICO meeting on Care.Data- 19th September 2013

Dear All

Please find attached the final paper for tomorrow's meeting - the PIA. Please note that this is an early draft and intended to be an update on progress rather than a final version.

See you all tomorrow at 11.15am

Thanks  
Rachel

.....  
.....

This message may contain confidential information. If you are not the intended recipient please inform the sender that you have received the message in error before deleting it. Please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents: to do so is strictly prohibited and may be unlawful.

Thank you for your co-operation.

NHSmail is the secure email and directory service available for all NHS staff in England and Scotland  
NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and GSi recipients  
NHSmail provides an email address for your career in the NHS and can be accessed anywhere

.....  
.....



# Privacy impact assessment:

## Care.Data Programme

Version 0.5

September 2013

Contents

Executive Summary

Why Privacy Impact Assessment

What is care.data?

Privacy issues as a consequence of care.data

Business case – context, benefits, and implications

Alternatives to identifiable data

What we will do to protect privacy?

Public acceptability

Conclusions

Appendices

A - Managing Privacy Risk

(i) - Types of privacy risk

(ii) - Risk Mitigation Matrix

B - Examples of use

C - Definitions of terms

D – Further information

## 1. Executive Summary

1. NHS England (formally the NHS Commissioning Board [NHS CB]<sup>1</sup>) was established on 1 October 2012 as an Executive Non-Departmental Body.
2. NHS England aims to ensure high quality care for all, now and for future generations. We are committed to transparency and to putting patients and the public at the heart of all decisions, grounded by the values and principles of the NHS Constitution. The responsibilities of NHS England can be divided into the following domains:
  - Reducing mortality
  - Improving care for patients with long term conditions
  - Improving acute care
  - Improving patient experience
  - Improving patient safety
3. Care.data will bring together securely, health and social care information from all care settings in order to improve the quality, efficiency, and equity of services. For the first time, it will allow nationwide linkage of primary and secondary care data in order to identify any unwarranted variations in care across the country. Care.data will enable increased use of information that the NHS already collects with the intention of improving healthcare, by ensuring that timely and accurate data are made available to NHS commissioners, providers, and researchers.
4. Under the Health and Social Care Act 2012, NHS England can direct the Health and Social Care Information Centre (HSCIC) to collect data from every provider of care funded by the NHS. This limited to where the data are necessary for exercising the functions of NHS England. These data are collated, stored, and disseminated or published by the HSCIC rather than NHS England. The HSCIC provides a secure data environment, which operates to the very highest technical and security standards. The HSCIC will disseminate data in three formats:
  - 1) Anonymous or aggregated data will be published in line with Information Commissioner's Office (ICO) guidance without risk of identification and with small number suppression.
  - 2) Pseudonymised<sup>2</sup> data will be disclosed by the HSCIC to specific groups of users, initially for commissioning uses only and in line with ICO guidance.
  - 3) Identifiable data will be where there is a legal basis for doing so (e.g. with patient consent or approval under section 251 of the NHS Act 2006).
5. A privacy impact assessment (PIA) is a tool, process or method to identify, assess, mitigate or avoid privacy risks. This PIA describes how data will be collected, processed, disseminated and published for care.data. It explains what the programme will do to protect privacy and the solutions that have been identified and implemented to help safeguard privacy. This document will enable readers to assess for themselves what may be considered a potential impact on their privacy.

---

<sup>1</sup> NHS England is the operating name of the NHS Commissioning Board as established by the Health and Social Care Act 2012. It is referred to throughout this document as NHS England

<sup>2</sup> The process of distinguishing individuals in a dataset by using a unique identifier, which does not reveal their 'real world' identity. The NHS number and other identifiers, are replaced by a key.

- e. The HSCIC has undertaken a privacy impact assessment for all the personal data it processes, which includes the data extracted for care.data.<sup>3</sup> This privacy impact assessment specifically considers the privacy impact of care.data in greater detail.

## 2. Why privacy impact assessment?

Privacy impact assessments (PIAs) were launched in the UK by the Information Commissioner in December 2007 and were mandated by the Cabinet Office for information and communications technology (ICT) projects following the Data Handling Review of June 2008<sup>4</sup>.

The Health and Social Care Act 2012 introduces legislative powers that enable NHS England to direct the HSCIC to obtain and process identifiable patient data in certain circumstances without the need for patient consent. This arrangement includes care.data. Patients, and those people legally empowered to act on their behalf, must be informed about how identifiable data about them are used. Therefore, alongside other awareness-raising activities, NHS England and the HSCIC are informing patients about how care.data might affect the privacy of personal data. The privacy impact assessment:

- Describes the purpose and objectives of the care.data programme;
- Assesses the potential implications for privacy; and
- Explains what NHS England and the HSCIC will do to protect privacy.

The scope of this PIA covers the whole of the care.data programme, including each of the domains of health and social care information that are currently planned to be included within the programme. The care.data programme has a number of phases relating both to the data sets to be acquired and the functionality offered. All of these phases are encompassed by this PIA. The PIA will be kept under review and revised as the detail for each phase is developed.

## 3. What is care.data?

The care.data programme is a major upgrade of the Hospital Episodes Statistics (HES) service that will link a more complete range of data at record level across England. It will collect, collate and link clinical and other data from all health and care settings, including hospital, primary care, community, mental health and social care. The combined datasets will be made available to others in a range of formats, with all appropriate safeguards in place to protect confidentiality.

Specifically, the programme's objectives are

- patient safety
- improve outcomes

---

<sup>3</sup> [\[INSERT LINK TO HSCIC PIA\]](#)

<sup>4</sup>

[http://www.ico.org.uk/about\\_us/consultations/-/media/documents/library/Corporate/Research\\_and\\_reports/pia-executive-summary.pdf](http://www.ico.org.uk/about_us/consultations/-/media/documents/library/Corporate/Research_and_reports/pia-executive-summary.pdf)



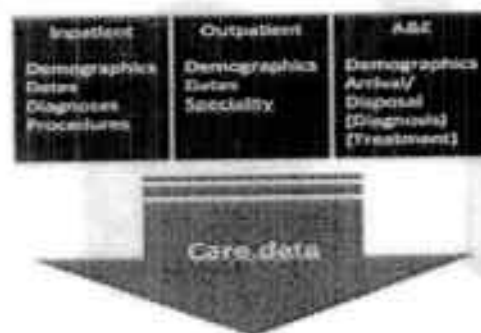
- reduce waste
- minimise health care inequalities
- remove unwarranted variation
- empower citizens and staff; and
- deliver high quality health care for all.

Currently, health and social care data are not joined together in order to provide a complete view of the patient journey. This makes it difficult or impossible to assess the safety, effectiveness and efficiency of health and care services. To address these shortcomings, care.data will collect and link data from different health and social care settings.

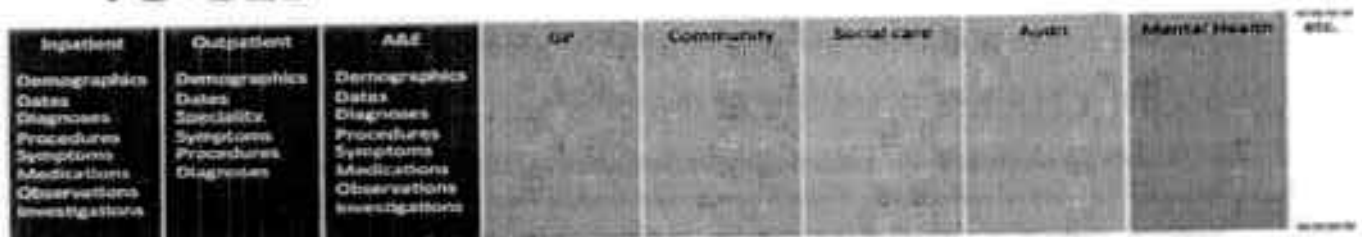
For many years, data have been collected from all hospitals providing NHS care. This dataset, HES, has been used for tens of thousands of research studies and clinical audits. However, by definition, HES is limited to hospital data whereas the bulk of NHS care episodes occur in community settings. As a result, commissioners are often unable to ensure that joined-up care is being provided to their patients.

The care.data programme is designed to ensure that commissioners have access to a dataset that contains linked information from all GP practices and all hospitals. Over the following years, data will be progressively added from all other care settings, including community health services and social care, and the hospital dataset itself will become much richer and more complete. This transformation will see Hospital Episode Statistics (HES) evolve into a care episode service (CES).

## From HES



## To CES

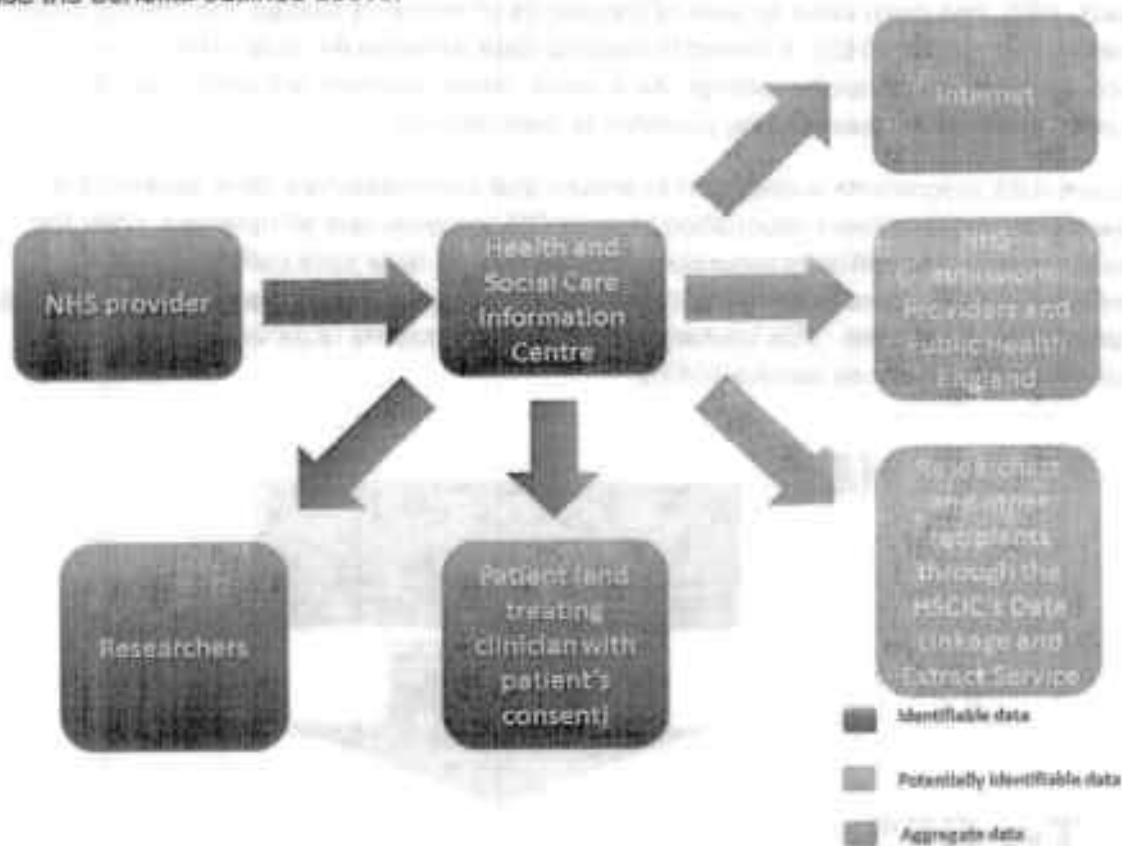


The HSCIC will collect and process the data for care.data using its powers under the Health and Social Care Act 2012. The HSCIC is England's central, authoritative source of health and social care information. The HSCIC will process patients' confidential data in a secure environment and will only release confidential data where there is a legal basis for doing so.

The main functions of the HSCIC in relation to care.data are to:

- i. collect and process, patient identifiable data extracted from patient records;
- ii. assure the data quality of patient identifiable data;
- iii. link and de-identify patient identifiable data;
- iv. publish aggregate data;
- v. disseminate potentially identifiable data to approved bodies and where strict controls exist so the likelihood of an individual being identified are very small;
- vi. disseminate to specific bodies patient identifiable data (only where necessary, in exceptional circumstances and when lawfully authorised e.g. under section 251 of the NHS Act 2006). This is a future aim and subject to independent approval.

The following diagram shows how the linked dataset will be made available in order to realise the benefits outlined above.



The privacy impact of these data flows is considered in further detail below.

#### 4. Privacy issues as a consequence of care.data

This section assesses the potential impact on privacy of care.data. To assess the potential privacy impact of care.data, it is necessary to weigh up not only whether the impact is positive, neutral or negative but also to consider the extent to which any adverse impact on privacy may be acceptable if it brings other benefits. Safeguards to protect privacy are explained in Section 7.

Care.data involves the extract of personal confidential data from health records, including *sensitive personal data* as defined in the Data Protection Act 1998. Identifiers (NHS

number, date of birth, postcode and gender) are extracted from providers together with coded clinical information and sent to the HSCIC. As with any disclosure of personal confidential data, there are associated risks to privacy and confidentiality.

The privacy impact can be considered in three areas:

- The extraction of personal confidential data into the HSCIC
- The processing of the personal confidential data when held by the HSCIC
- The onward disclosure of data from the HSCIC

#### **(i) The extraction of personal confidential data into the HSCIC**

The Health and Social Care Act 2012 provides a legal basis for the extraction of personal confidential data in certain circumstances. The Act sets aside the requirement under the common law duty of confidence to seek patient consent<sup>5</sup>. Certain requirements under the Data Protection Act 1998 continue to apply – in particular, the fair processing principle, which means that patients must be made aware of how confidential data are processed for care.data.

The extraction of personal confidential data from providers without consent carries the risk that patients may lose trust in the confidential nature of the health service. This risk is two fold: firstly, patients will not receive optimal healthcare if they withhold information from the clinicians that are treating them; and secondly, that this loss of trust degrade the quality of data for care.data and other secondary uses of NHS data.

To mitigate against the risk, NHS England has committed to giving patients the right to object to personal confidential data leaving their GP practice and, in general, to having their objections upheld in line with the commitment given by the Secretary of State for Health in April 2013<sup>6</sup>. Previously there was no mechanism for patients to exercise this right. This is therefore a step forward in enabling patients greater control over the identifiable information held about them. Personal confidential data have been processed for many years where there has been a legal basis for doing so (e.g., where there is special approval for research). This new objection extends to all disclosures of personal confidential data from the GP practice, not just care.data.

In order to ensure that patients are aware of the changes to how data are processed for care.data, and to ensure they are aware they can object, a number of awareness raising activities will be undertaken. Figure 1 summarises the awareness raising activities that are taking place.

---

<sup>5</sup> Under Sections 259 and 256 of the Health and Social Care Act 2012

<sup>6</sup> At the launch of the Caldicott Information Governance Review Report 26 April 2013

### Figure 1 - Summary of supporting activities and resources

- A patient leaflet and poster about information sharing made available in GP practices
- Materials developed in accessible formats including Braille, large print and audio versions.
- Materials for GP practices to support patient awareness raising including a how to guide and a template press release for local tailoring
- Detailed FAQs for both GPs and patients
- Testing of these materials in a limited number of GP practices with feedback incorporated into the national version of the leaflet and poster.
- A mailing of a leaflet about information sharing to every household in England
- Separate GP and patient information lines to support understanding
- Social and digital media: dedicated web support pages for patients through NHS Choices and for professionals through NHS England.
- Use of central social media channels to help raise awareness and to direct to particular FAQs such as objection process.
- Engagement with a number of national patient groups, charity and voluntary sector organisations to enable cascade of messages through their regular and social media channels.

In order to evaluate the potential impact on their privacy, patients need to understand what data are to be extracted. As explained above in section 3, the first stage of CES will involve linking GP data to hospital data. Data from other parts of the health and social care service will be linked over time. The dataset extracted from GP systems has been published<sup>7</sup> and includes data such as referrals, prescriptions, symptoms, diagnoses, and treatments. Whilst all health data is classified as sensitive personal data under the DPA, a list of particularly sensitive items will be excluded from extracts<sup>8</sup>. The data extracted is in the format of a series of codes. Free text (i.e., words, sentences, and paragraphs) will not be extracted for care data.

Extraction of the GP data will be on a monthly basis, prospective from April 2013, using the General Practice Extraction Service (GPES). This is a tool provided by the HSCIC, which extracts data from GP practices into the HSCIC. The GP dataset has been considered by an independent group of clinical informatics experts, which included representatives from the British Medical Association (BMA) and the Royal College of General Practitioners (RCGP). The group was satisfied that the dataset seemed appropriate for commissioning. Any future changes to the dataset or to its scope will be subject to further review by the group. In addition, the care.data proposal was also reviewed and approved by the GPES Independent Advisory Group (IAG), which include clinical and patient representation. Any changes or updates to the dataset will be published on the NHS England website.

<sup>7</sup> <http://www.england.nhs.uk/wp-content/uploads/2013/08/cd-ces-tech-spec.pdf>

<sup>8</sup> <http://www.england.nhs.uk/wp-content/uploads/2013/08/cd-ces-tech-spec.pdf>

Reasons for processing and benefits	Impact on privacy	Controls and Pledges
<ul style="list-style-type: none"> <li>Personal confidential data are extracted from healthcare providers to enable linkage.</li> </ul>	<ul style="list-style-type: none"> <li>Some people may feel a loss of individual autonomy (no patient consent)</li> <li>Some patients not be aware of or understand their choices.</li> <li>Awareness raising activities will help patients understand how their data are used not only for care data but other uses of healthcare.</li> </ul>	<ul style="list-style-type: none"> <li>Statutory basis for data collection required or permitted by law<sup>9</sup></li> <li>Identifiable data must be necessary to satisfy the purpose</li> <li>Patients can object to the processing of the personal confidential data in GP records.</li> <li>Patients can change their mind at any time and identifiers can subsequently be removed from the HSCIC</li> <li>Control 1 (see Section 7 – “Information Governance Controls”)</li> <li>Pledge A, B, C, D and E (see section 7 – “Additional care data pledges to protect information”)</li> </ul>

**(ii) The processing of the personal confidential data when held by the HSCIC**

The HSCIC’s PIA details the risks and responsibilities it has to protect the confidentiality of all the data it holds. This PIA is much broader than care data PIA because the HSCIC is the data controller for numerous datasets in addition to care data. The HSCIC PIA covers the responsibilities the HSCIC has including guarding against risks and threats from inside and outside the organisation. The risks described include threats associated with ‘cyberspace’ such as hackers attempting to access the data illegally.

The HSCIC will process the personal confidential data for the care data service. This arrangement has a potential impact on privacy because the HSCIC is an organisation, to which the patient has not disclosed information themselves. There are also known privacy implications with centralised data collections (e.g., in relation to ensuring the relevancy of the data extracted).

At a local level, personal confidential health data have been used for many years for the purposes of indirect care (e.g. for planning services, audit, and research). There have been incidents of local data breaches and also a misunderstanding of the complex legal and

<sup>9</sup> The Health and Social Care Act provides powers for the Health and Social Care Information Centre to require organisations to submit data to it when data collection has been mandated by NHS England or Secretary of State, and in some circumstances, where requested by other bodies.



information governance framework for health data. Local processing can be difficult to monitor and audit, and the likelihood of an individual being identifiable when processing takes place locally is higher than when data are processed centrally (e.g. recognising the name of a neighbour). Whilst a centralised data collection has potential privacy implications, these risks can be balanced with a reduction in the requirements for local processing of personal confidential data and with assurances that data processing by the HSCIC is to the highest security standards. The technical expertise and detailed knowledge of information governance is very difficult to match across all organisations operating at a local level.

It is necessary for the HSCIC to receive identifiers so that it can link data from different healthcare settings to realise the benefits outlined in section 5. Data linkage involves matching together the records from two or more care settings about the same patient to provide a more complete picture of the patient's needs, experiences of care, and outcomes. For example, hospital records and general practice records could be linked in order to analyse the impact upon outcomes of different care pathways for a particular condition.

The privacy risks associated with the HSCIC are mitigated because the process of linking the record is automated. Occasionally, in a small number of cases, it is necessary for HSCIC analysts to check the data for data quality reasons. However, this human involvement is done following strict rules and processes, all of which are designed to protect the confidentiality of the individual. These include, for example, rules around keeping the data, destroying the data, disclosing the data and illegally matching data to identify individuals.

It is important to reiterate that the data that the HSCIC processes for care data do not include patients' names and addresses. Furthermore, the data are presented in terms of clinical codes rather than free text (i.e., no words, sentences, or paragraphs). Once the record has been linked, the identifiers are removed so a new record is created that does not identify the patient.

Where patients have objected to the flow of their personal confidential data from the general practice record, the HSCIC will receive clinical data without any identifiers attached (i.e. anonymised data).

If a patient objects to flows of personal confidential data from the GP practice and from the HSCIC (see 4 iii) then it is necessary for the patient's NHS number to flow to the HSCIC so that the HSCIC is aware of this objection and can stop personal confidential data it holds from other care settings leaving the HSCIC. This has been described to patients in FAQs.

Reasons for processing and benefits	Impact on privacy	Controls and Pledges
<ul style="list-style-type: none"> <li>• Accuracy has to be checked before data are de-identified (it is not possible afterwards)</li> <li>• Linking data from different healthcare settings in order to deliver a linked dataset to commissioner and other</li> </ul>	<ul style="list-style-type: none"> <li>• Data collection, storage and processing creates risk of confidential information being accessed without knowledge or consent of patient</li> <li>• De-identifying data reduces or eliminates</li> </ul>	<ul style="list-style-type: none"> <li>• Statutory basis for collection and analysis.</li> <li>• Identifiable data stored only where necessary and destroyed or effectively anonymised as soon as no longer necessary</li> <li>• Approval from an</li> </ul>

<p>approved bodies.</p> <ul style="list-style-type: none"> <li>De-identification so that the data can be used more freely for the benefit of the health service.</li> </ul>	<p>the risk of a person's identity being revealed and thus helps protect privacy</p> <ul style="list-style-type: none"> <li>Risks in terms of changes to scope without patients being aware.</li> <li>Extraction once at national level reduces the need for local processing of personal confidential data where patients are more likely to be identifiable or where the safeguards in place, may not be as robust.</li> </ul>	<p>Independent Advisory Group for any changes in scope and publication of this information.</p> <ul style="list-style-type: none"> <li>Controls 2, 3, 4 and 7 (see Section 7 – "Information Governance Controls")</li> <li>Pledges B, C, D, E and F - (see section 7 – "Additional care data pledges to protect information")</li> </ul>
---	--	--

### (iii) The onward of disclosure of data from the HSCIC

The law pulls in different directions where dissemination of information is concerned; Human Rights and Data Protection legislation, along with our domestic common law duty to respect confidentiality, require us to protect information that could identify an individual. The Freedom of Information Act encourages publication and availability of public information although also balancing this with the requirement to protect personal data. The Health and Social Care Act 2012 allows the HSCIC to obtain and disseminate information about patients under direction, again whilst balancing the need to protect the identity of individuals.

The diagram on page 6 shows how data will be made available from the HSCIC. There are three categories of disclosure:

- Green flow – aggregate data
- Amber flow – potentially identifiable data
- Red flow – personal confidential data

Green flows of data will be published only in aggregated form without risk of identification. This will be in line with the ICO code of practice on anonymisation and the Information Standards Board anonymisation standard for publishing health and social care data.

Amber data will only be disclosed by the HSCIC to approved specific groups of users such as commissioners and possibly in the future, approved researchers. Amber data is pseudonymised i.e. identifiers such as the NHS number are replaced by a unique identifier, which does not reveal real world identity. Although there is limited risk that the data is potentially identifiable (i.e. due to a rare disease) if it is processed in a controlled environment it is considered anonymised in line with the ICO code. Therefore all amber

disclosures will be in accordance with robust information governance controls for example, a legally binding contract.

Whilst there is privacy risk that those granted access to these pseudonymised flow could potentially misuse the data by re-identifying patients by combining the pseudonymised data with other available datasets (this is known as a jigsaw attack) the chances are remote and such an attack would be illegal and therefore subject to sanction by the ICO. A key safeguard to prevent this is to provide such data under contract with requirements that there is no onward disclosure of the data.

**Red Flows** – These involve the disclosure of personal confidential data from the HSCIC. This is only permitted where there is a legal basis for example, explicit patient consent, approval for research under section 251 of the NHS Act 2006 or exceptionally where there is an overriding public interest in disclosure such as an outbreak of a new disease or a civil emergency. In order to establish trust in care data from patients and healthcare professionals, personal confidential data collected for care data will initially only be disclosed where there is an overriding public interest even though disclosures under section 251 or with patient consent would be legally permissible.

If it is decided in the future that personal confidential data, collected as part of the care data programme, will be disclosed by the HSCIC e.g. where there is section 251 approval, patients can object to this by informing their GP who can enter a code into the GP record. This code prevents personal confidential data from any healthcare setting leaving the HSCIC unless there is an overriding public interest such as a civil emergency. Whilst it is possible for patients to object to the processing of personal confidential data under section 10 of the Data Protection Act 1998, this new code allows patients to exercise, to a large degree, choice by simply having a code entered into their GP practice record. Put simply, patients who are concerned about their privacy can control the flow of confidential data from GP practices AND flows of personal confidential from any healthcare setting leaving the HSCIC.

Reason for processing and benefits	Impact on privacy	Controls and Pledges
<ul style="list-style-type: none"> <li>• Once data are de-identified they can be used without breaching confidentiality for a large number of "secondary purposes" that are fundamental to the operation of the NHS and/or necessary to improving public health or health and social services where jointly commissioned with the NHS.</li> <li>• Data are used to inform commissioning decisions for example to understand patient pathways, need and most effective provision.</li> <li>• Data are used to understand the outcomes for patients of the care they receive for patient experience and</li> </ul>	<ul style="list-style-type: none"> <li>• In some cases, a small residual risk that identifiable data could be revealed</li> <li>• Risks may increase as more effectively anonymised data are made available, and to more organisations (both public and non-public) i.e. a risk of matching datasets to reveal identity.</li> </ul>	<ul style="list-style-type: none"> <li>• No constraints for use of published statistics or reports</li> <li>• Restrictions on re-use apply in other circumstances</li> <li>• Patients can object to their personal confidential data leaving the HSCIC.</li> <li>• Controls 5, 6, 8 (see Section 7 – "Information Governance Controls")</li> <li>• Pledges B, C, E, F; (see section 7 – "Additional care data pledges to protect information")</li> </ul>



<p>efficacy.</p> <ul style="list-style-type: none"> <li>• Information used by the public to make health care decisions, and by people inside and outside the NHS for activities such as medical research, public health and national clinical audit, has to be of a good quality.</li> <li>• Benchmarking care provision in order to identify outliers and take action to improve services using the lessons learnt from those performing well on those performing less well</li> </ul>		
---	--	--

## Conclusions

The main concern within this assessment is the balance between the benefits of linked personal confidential data in the form of health and social care records being processed in order to improve care provision through improved commissioning, outcomes focus, performance monitoring and research against the risks to patient privacy of undertaking this. A key component of any assessment is the strict controls and security that will be applied to these data by the HSCIC such that only the HSCIC will process data in identifiable form which limits the risks of the privacy of individuals being breached by this programme. A potential positive impact of care.data is that more organisations should be able to make use of effectively anonymised information provided by the HSCIC rather than using identifiable information.

The potential risks to privacy from care.data are:

- A. Loss of individual autonomy from use of patient data without consent
- B. Risk of confidential information being accessed and viewed without knowledge or consent of patient
- C. Linking and de-identification processes may not be reliable enough to achieve total anonymisation of data
- D. Risk of data being accessed illegally and then sold or otherwise misused by commercial organisations; and
- E. Risk of data being accessed legally and then the data being misused.

The actual impact on privacy will be mitigated by a full range of controls which care.data will use to safeguard the identifiable information it uses – discussed in section 7.

## 5. Business case

This section provides the business case for care.data. It explains why NHS England believes that these changes are so important and the value that the linked pseudonymised data and published aggregate data can bring to patients, the public, health and social care providers, commissioners, researchers. It also describes the positive impact these developments could have on the economy.

### Context

Health and care providers collect vast quantities of data through millions of interactions with patients every week and yet most providers of care struggle to evidence the benefits of the treatment they give to patients. There are no systematic mechanisms to link health and social care data from various settings such as primary, secondary, community and social care on a national basis. This results in an inability to look across the true patient care pathway except for in a few geographical areas or across a limited number of systems. In addition, inconsistencies or inaccuracies in the data captured, combined with difficulties in accessing the data, has meant that this potentially rich resource has generally been under-used.

Care.data will bring together data from these various settings and systems to deliver national coverage and an ability to look across all pathways, providers and conditions. The care.data programme will unlock the potential of data by creating an environment where data flow more effectively and the true outcome of any interventions can be understood. The ability to link data from different sources will enable new and exciting possibilities for the monitoring of outcomes, and also for identifying early indicators of the risk of developing certain conditions. The insights derived will help drive local innovation, building clinical commitment to gathering data and public confidence in the services used. Clinicians will be directly involved in agreeing what key data are required to produce meaningful intelligence. The GP dataset, for example, has been reviewed by a clinical expert group (as described on page 8) and there has been a national consultation on the hospital dataset. In the future, patients will have ready access to the same information. NHS England will work with information intermediaries to encourage the development of more accessible ways for patients to use these data to inform choices about their care and wellbeing.

### Better commissioning and services to patients

Successful local and national commissioning in the new health and social care system is highly dependent upon creating ready access to high quality information that can be derived from these streams of data. The capture and linkage of this person-centred health and social care data will support the commissioning and delivery of services based upon pathways of care, resulting in more cohesive, joined up services and better outcomes for patients (e.g. through informed interventions, better resource allocation, performance incentives). Intelligence gained from the linked data can ensure that only the best, and most appropriate, services get commissioned.

### Research benefits

It is intended that care.data will provide information to enable research, public health surveillance, clinical audit and other important purposes that are fundamental to improving health care. This can best be illustrated by example.

Consider a patient with lung cancer attending a hospital outpatient clinic in order to receive chemotherapy. The patient's treatment relies upon use of patient-related data for a host of medical purposes including:

- Decades of research into the most effective interventions for that form of cancer, including:
  - I. Clinical trials of each constituent drug in the cocktail of drugs they are receiving in that chemotherapy regime, and each of the sub-optimal alternative drugs not being used, so that results and side-effects can be identified.
  - II. Clinical trials into different combinations of potential drugs, in different doses, administered in different frequencies through different methods in order to test potential chemotherapy regimes.
  - III. "Desk-based research" to assess evidence from around the world of outcomes of clinical trials and actual treatment using different chemotherapy regimes.
- National clinical audit to check that cancer care is being provided as intended;
- Review of patient-reported experiences to identify how to provide care to improve outcomes;
- Reporting to Public Health England and predecessor organisations through the "yellow card scheme" of adverse reactions of other lung cancer patients to chemotherapy regimes;
- Analysis by the National Patient Safety Agency of cases of misdiagnosis of lung cancer;
- Surveillance by local authorities and other public health agencies to identify high-risk target groups that might benefit most from "stop smoking" campaigns, and assess different methods of conveying the public health message effectively;
- Work by commissioning organisations to assess, commission and monitor the chemotherapy service provided by the acute trust;
- Inspection of the acute trust and its services by the Care Quality Commission;
- Responses by the trust to previous complaints from patients receiving lung cancer services;
- Review of trust performance figures by the GP referring the patient; and
- Review by the acute trust oncology service manager of previous out-patient clinic appointment lengths for similar patients to plan and schedule the timings and skill-mix required for appointments in the clinic; and
- Reporting and monitoring of waiting times to meet targets for cancer patients.

Whilst none of the above activities involves the care of an individual patient, they are all

fundamental to the lung cancer patient's care. All depend upon access to effectively anonymised data derived from the confidential information within patient records. A major role of care data will be to provide such information.

Further examples are included in Appendix B.

### **Informed Choices**

Better information and access to information will give patients the opportunity to exercise control over their needs and choices and to inform choices about their care and wellbeing (e.g. visible choice, shortest waits).

Liberating the NHS: An information strategy lists the kinds of information that people will use, including:

- suitable medicines, treatments, and any risks, benefits and side effects;
- clinical outcomes and success rates, such as readmission or mortality rates;
- other indicators of quality and performance, such as infection rates.

An important role of care data is to provide such information, and enable patients to make informed choices and play their part in making a more effective, efficient health service. NHS England, through care data will be proactive, encouraging people to make use of information it publishes. It must also be responsive; providing information that people say they want in the form they want it.

### **Greater accountability**

Making care data available will enable citizens to better hold the NHS to account in relation to many areas such as the extent of equitable provision of drugs across England and the achievement of waiting and other targets.

### **Greater efficiency**

Analysis of data can help improve efficiency for example:

- Easier, quicker access to better information can drive improvements in professional approaches and ways of working. The ability to identify variances and inconsistencies in services, for example, in prescribing and pathology services or in slot availability, will help increase productivity.
- Information that supports current and emerging commissioning and NHS-wide performance management information needs supports organisations to deliver service improvements and measurement of performance and quality and will help reduce local commissioner and provider processing costs.

### **Economic Growth**

Care data will support economic growth for example:

- Greater access to health and care data and its open publication will help reinforce the UK as a global centre for life science research. Making anonymous data available at scale will help researchers discover and refine new treatments and shed light on connections between, for example, health outcomes and social conditions.



- Facilitating transparency and openness by providing open access to secondary uses and comparative data for a wide range of users supports the development of a vibrant market place.
- Offering a range of core national services to enable the potential for additional services at a sub-national or local level supports economic growth through the involvement of SMEs in the future provision of innovative analytics tools and services. It also provides the potential to use new commercial vehicles to commission services in a cost-effective manner.
- Enabling the visibility of 'postcode prescribing' and variable/inequitable provision will support social growth.
- The economic growth agenda will be supported by better information supporting the modernisation of services and being able to identify areas of service shortfall for new entrants.

### Improved Governance

The care.data programme is underpinned by a strong governance structure, which includes the delivery organisation (HSCIC). The care.data programme will combine a number of existing and emerging programmes, bringing together key stakeholders to ensure that appropriate controls and information governance is in place; that risks and issues are managed; that requirements are met; that the direction of the programme is clear and consistent; and that the benefits of the programme are fully realised.

Oversight of the care.data programme will be through the care.data programme board, which includes an engagement, stakeholder relations and communications management workstream. This workstream is responsible for oversight of the stakeholder engagement strategy and for co-ordinating and overseeing the delivery of this strategy.

### 6. Alternatives to identifiable data

As can be seen from the business case the key purpose and benefit of care.data is to link health and social care datasets in order to provide a linked continuum of the patient pathway. This is the closest approximation to what a patient experiences so that we may improve care provision and outcomes. For example true patient outcomes may be assessed routinely, so rather than knowing that a patient has been discharged following a hip operation it is possible to know whether they have maintained independence.

This continuum may only be achieved through linked data, in turn data may only be linked by the use of a common and consistent identifier across the information. The identifiers used for linkage are NHS number, date of birth, gender and postcode. Alternative data linkage through the use of weaker identifiers has been rejected due to two risks:

- The scale of the linkage required i.e. for all patient records from a range of health and care settings.
- Incorrect linkages are made causing data accuracy issues and therefore bringing into question any of the uses of care.data
- A low proportion of linked records bringing into question the validity of any use of care.data as either not representative or containing a bias of records able to be linked or that are not linked.

Because the care settings, information systems and data sets to achieve this continuum are so diverse and are not integrated, care data through the HSCIC requires identifiers to be able to accurately link this information.

The alternative is to link information systems at source and provide a common anonymous key from the source systems to allow linkage. This is considered impractical as there are such a diverse number of care settings (primary, secondary, community social care) and a diverse number of information systems that this would not be achievable or the most effective method to achieve the goals of improving patient care.

## 7. What will we do to protect privacy?

This section explains what we will do, with the HSCIC as the delivery partner, in order to safeguard patient privacy.

It should be recognised that the HSCIC has been processing patient records safely and securely since its inception. It has introduced strong security controls, published and implemented security policies and published information about its processing as required for compliance with the Department of Health's Information Governance Framework.

The HSCIC takes its responsibilities as a custodian of patient information extremely seriously and is also committing to a number of pledges to protect privacy as set out below.

Appendix A shows how the privacy risks identified in section 4 are addressed by the information governance controls and pledges below.

### Information Governance Controls

The HSCIC will collect, process, disseminate and publish data on behalf of NHS England for and care data. The Health and Social Care Information Centre will:

- 1) Obtain and process the minimum necessary identifiable patient data from other organisations;
- 2) Store and process identifiable data securely, meeting or exceeding the standards required of NHS organisations, including technology to:
  - i. De-identify data received as early as possible, and where records have to be linked, separate patient identifying data from clinical data, and assign a meaningless identifier
  - ii. Store data in a "accredited safe haven"<sup>10</sup> capacity
  - iii. protect against attacks from unauthorised individuals (e.g. hackers)
  - iv. protect against careless or negligent behaviour by staff (not logging off thereby leaving confidential data visible on computer screens);

---

<sup>10</sup> An accredited organisation with a secure electronic environment in which personal confidential data and/or de-identified data can be obtained and made available to users, generally in de-identified form.

- v. provide only legitimate personnel with access to Health and Social Care Information Centre systems, and to no more access than they require;
  - vi. protect against staff from giving themselves rights of access to Health and Social Care Information Centre computer systems;
3. Keep to the absolute minimum the number of staff able to access and view patient identifiable data, and wherever practicable assign staff rights of access to either patient identifiers or clinical data and not both;
  4. Destroy data held in identifiable form as soon as it is no longer necessary, or in accordance with the retention policy;
  5. Disclose only effectively anonymised data, other than:
    - i. with explicit patient consent;
    - ii. where required by statute, or
    - iii. where allowed by statute, or exceptional public interest, as permitted by section 261 of the Health and Social Care Act 2012 with necessary support and approvals, and either:
      - the support of the Independent Advisory Group; or
      - where urgent, with the agreement of both the Senior Information Risk Officer and Caldicott Guardian for NHS England;
  6. When disclosing effectively anonymised data, restrict the data disclosed according to the context in which the data will be used:
    - i. When publishing statistics and other aggregated information, apply disclosure control standards to ensure data are effectively anonymised;
    - ii. When disclosing patient-level data to a trusted organisation:
      - confirm the data are effectively anonymised by carrying out a risk assessment
      - maintain a written agreement with the recipient organisation that stipulates the allowed access and uses of the data;
  7. Monitor who accesses patient identifiable data.
  8. The Health and Social Care Information Centre provides assurances regarding Information Governance through satisfactory completion of the NHS Information Governance Toolkit . This encompasses:
    - Staff training and contracts
    - information technology system security and audit trails
    - Robust management arrangements
    - Full compliance with legislative requirements

## **Additional care.data pledges to protect information**

In addition to the information governance best practice outlined above, NHS England and the HSCIC are implementing further safeguards in place to protect information and will be held to account against these pledges by the Department of Health. NHS England and HSCIC will:

- A. Establish an Independent Advisory Group to monitor governance of identifiable patient data, and act on its advice;
- B. Publish a Code of Practice to govern the use of confidential data supplied to the Health and Social Care Information Centre that encompasses care.data;
- C. Respect the wishes of patients who request that their data are not used by care.data, unless there is a statutory duty or an overriding public interest (e.g. public health emergency) to do otherwise;
- D. Commission, at least annually, external information governance audit against information governance standards.
- E. Be transparent about its activities and communicate openly, fairly and lawfully through the relevant sections of the NHS England and HSCIC public websites and other channels where appropriate;
- F. Publish procedures for dealing with requests for information and operate effective policies and procedures to encourage good information governance by staff, with proportionate sanctions (e.g. dismissal) for inappropriate or negligent behaviour.

## **8. Public Acceptability**

Personal confidential data have been used for purposes beyond direct care for many years for example, for healthcare planning and for research. It is important that patients are clear about what information is being shared, how and why so that they can understand the benefits to them and the wider population. Some patients may have concerns, for personally valid reasons and therefore NHS England has made it easy for patients to object.

The General Practice Extraction Service Independent Advisory Group (IAG), which includes lay representation approved the extraction of GP data in order for it to be linked to hospital data and made available to commissioners.

NHS England and the HSCIC have worked closely with the British Medical Association and the Royal College of General Practitioners during this process and listened to and incorporated views culminating in joint guidance and materials for GP practices. The BMA's Patient Liaison Group (PLG) was involved in commenting on the patient materials.

Care.data was piloted in a small number of practices over the summer. GP practice staff and patients were invited to feedback on materials and NHS England communicated with the first practices in order to gauge public acceptability at this early stage. Dialogue will continue with these practices as care.data is implemented on a national scale.

Information about the programme has been sent to over 350,000 patient groups, charities, and voluntary organisations. These organisations are being asked to cascade information about care.data to their members through their usual channels, including social media. NHS



England has been engaging with the strategic partnership programme<sup>11</sup>, which enables voluntary sector organisations to work in equal partnership with the Department of Health (DH), NHS and Social Care to help shape and deliver policies and programmes. A series of meetings are being set up with patient groups to discuss care.data. Meetings have been held with stakeholders for example Cancer Research UK. This is an ongoing exercise and further meetings will take place over the coming weeks with patient groups and charities to discuss and seek views on the long term vision for care.data.

## 9. Conclusions

Any processing or storage of identifiable patient data introduces potential risks of data misuse or breaches of privacy.

Although they can never be eliminated, such potential risks are significantly mitigated by robust information governance controls as set out in section 7 which are designed to safeguard patients' privacy. The commitment of care.data to meet or exceed all information governance standards provides greater assurance than most organisations are able to provide.

Furthermore, there is also a positive impact on privacy resulting from care.data de-identifying data. Making effectively anonymised data available, to commissioners, researchers and other approved bodies eliminates their risk of inappropriate use of identifiable data.

However, it is the case that processing information without the permission of the individual can be considered a loss of autonomy for that individual; although the extensive safeguards for the data have been well described.

In summary, those who conclude that the net impact on privacy will be positive are very likely to be supportive of care.data. Even people who feel the impact will be detrimental to privacy may recognise that the potential benefits of care.data using data from patient records are great, and may feel they are justifiable ethically on that basis. However, some people may believe that any use of patient identifiable data without explicit patient consent is unacceptable. These people are unlikely to be supportive of care.data whatever the potential benefits and may object to personal confidential data being used for wider healthcare purposes.

---

<sup>11</sup> <https://www.gov.uk/government/publications/the-department-of-health-voluntary-sector-strategic-partner-programme>

## **Appendix A - Managing Privacy Risk**

### **(i) - Types of privacy risk**

The Information Commissioner's Office Privacy Impact Assessment Handbook explains why privacy matters and identifies and describes four classes of privacy risk:

- privacy of personal information;
- privacy of the person;
- privacy of personal behaviour; and
- privacy of personal communications.

Care.data could potentially pose risks to the privacy of personal information i.e. the first of the bullets above.

Two categories of risk to the privacy of personal information are relevant:

- A. Risks to individuals as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information;
- B. Risks to organisations providing and/or using data within care.data as a result of:
  - I. perceived harm to privacy;
  - II. failure to meet public expectations on the protection of personal information (causing damage to the organisation's reputation);
  - III. failure to comply with the law, leading to enforcement action from the Information Commissioner; or compensation claims from individuals.

(ii) - Risk Mitigation Matrix

Section 4 identifies a list of potential privacy risks and potential impacts, and section 7 identifies information governance controls and pledges to reduce the risks to privacy. The table below indicates which risks each of the pledges is intended to address.

Control/Pledge to reduce risk/impact	Loss of autonomy	Confidential information viewed without consent	Misuse following illegal access	Misuse following lawful access
1) Obtain the minimum necessary identifiable data	√	√		
2) Store and process identifiable data securely		√	√	√
3) Minimise staff able to view identifiable data	√	√		√
4) Destroy identifiable data when no longer necessary	√	√	√	
5) Disclose only effectively anonymised data (other than lawful exceptions)	√	√		√
6) Restrict the data disclosed according to context e.g. whether or not published	√	√		
7) Monitor who accesses patient identifiable data		√		
A. Establish an Independent Advisory Group		√	√	√
B. Maintain agreements with data suppliers			√	√
C. Respect patient opt outs	√	√		
D. Commission information governance audits		√	√	√
E. Be transparent and communicate fairly and lawfully	√	√		
F. Operate good information governance amongst staff with sanctions for misconduct		√	√	√

**Appendix B – Examples of use [DN further work will take place to ensure that these are written in a way that is accessible to the public]**

**GP Data at the Nuffield Trust**

<p>New combined predictive models</p>	<p>Building on the commonly used Combined Predictive Model [1], the Nuffield Trust recently completed a programme of work to create updated and more powerful models to predict unplanned hospital admissions [2]. The resulting models relied heavily on GP consultations data in addition to linked hospital datasets.</p> <p>The study also helped extend our knowledge around the behaviour of such predictive models. For example, we tested the marginal benefit gained by adding GP variables, and found that predictive performance increased by several measures. In addition, the inclusion of GP derived variables specifically identified patients who were younger and less unwell. Such models may thus offer increased opportunities to target preventive care interventions to individuals who might be particularly receptive.</p> <p>[1] Combined Predictive Model: Final Report. Kings Fund, Dec 2006. <a href="http://www.kingsfund.org.uk/sites/files/kf/field/field_document/PARR-combined-predictive-model-final-report-dec06.pdf">http://www.kingsfund.org.uk/sites/files/kf/field/field_document/PARR-combined-predictive-model-final-report-dec06.pdf</a> (last accessed 04/06/2013)</p> <p>[2] Billings J, Georghiou T, Blunt I, Bardsley M. Choosing a model to predict hospital admission. An observational study of new variants of predictive models for case finding. <i>BMJ Open</i> (forthcoming 2013)</p>
<p>Whole systems demonstrator (WSD) trial</p>	<p>The Nuffield Trust led on one component of a large scale evaluation of telecare and telehealth assistive technologies [3,4].</p> <p>GP data were used in three ways:</p> <ul style="list-style-type: none"> <li>• To perform case mix adjustment between the trial's intervention and control groups. Combined model scores defined trial participants' risk of unplanned admission to hospital just prior to the assistive technology being installed.</li> <li>• To provide information on health measures of trial participants (eg Hba1c measurements, blood pressure readings, BMI scores etc).</li> <li>• To describe characteristics of the trial groups.</li> </ul> <p>[3] Steventon A, Bardsley M (2012). <i>The Impact of telehealth on use of hospital care and mortality</i>. Nuffield Trust, London.</p> <p>[4] Steventon A, Bardsley M, Billings J, Dixon J, Doll H, Hirani S, Cartwright M, Rixon L, napp M, Henderson C, Rogers A, Fitzpatrick R, Hendy J and Newman S (2012). 'Effect of telehealth on use of secondary care and mortality: findings from the Whole System Demonstrator cluster randomised trial', <i>British Medical Journal</i> 344: e3874</p>

Colorectal Cancer	<p>Colorectal cancer is the third most common cancer after breast and lung and a major cause of mortality. Patients' chances of survival at 5 years are much higher when colorectal cancers are detected at an early stage (93%) vs those diagnosed late (6%), however one quarter of colorectal cancer cases are diagnosed during emergency presentations.</p> <p>Using GP data linked to information from hospitals and the cancer registry, a study is in progress to examine variations in routes to diagnosis among patients with colorectal cancer in Outer North East London. The project will examine existing diagnostic pathways and aims to identify those that are best for the patient and have the minimum avoidable healthcare episodes.</p>
-------------------	---

University Hospitals Birmingham NHS Foundation Trust

#### Aims of the project:

- assess the level of healthcare usage in each healthcare system for the whole of England requiring all GP Extraction Service (GPES) data to link to HES to carry out deprivation and prevalence analysis of health system usage in terms of hospital care and primary care and judge survival for all disease groups for each system as to outcomes both quality and economic for high users of primary care compared to high users of secondary acute care.
- focus in on one specific disease group namely oesophageal cancer extend work on survival that has used HES and ONS by utilising primary care data.
- Advance an NIHR AQUITAK study tracking the outcomes of renal patients across the country. Looking at CKD stages, deprivation, types of treatment when access to treatment particularly cardiovascular.

The main objectives of this project are set as:

- Provide Business Intelligence (BI) tools for management of patients diagnosed with cancer in England. The BI tools will inform clinicians and managers on patients' pathways and related outcomes.
- Measure variations in patients' whole pathways and understand lessons from best practice.
- International comparisons: compare outcomes and treatments for cancer patients between US, England, Netherlands and Saudi Arabia.

There is a large body of evidence emerging from administrative datasets that shows geographical variations in cancer outcomes in England. ONS published statistics show that relative survivals vary widely by region ([http://www.ons.gov.uk/ons/dcp171778\\_262310.pdf](http://www.ons.gov.uk/ons/dcp171778_262310.pdf)). In addition, preliminary work carried out at University Hospitals Birmingham shows that for specific cancers there are variations in treatment and survival rates between secondary care providers.

#### Appendix C – Definition of Terms [DN to be added]

#### Appendix D – Further Information

Documents used in producing this PIA:

1. With thanks and reference to the Health and Social Care Information Centre Privacy Impact Assessment 'Functions of the Health and Social Care Information Centre' (Version of 17 July 2013)
2. Care.data Programme Definition Document v0.4 – 26 January 2013



**Iman Elmehdawy**

---

**From:** Dawn Monaghan  
**Sent:** 04 February 2014 11:19  
**To:** Jacob Smith  
**Subject:** Email from Rachel Merrett NHS England to Dawn Monaghan - 20131015  
**Importance:** High

For meridio

**Dawn Monaghan      Group Manager, Public Services**

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.  
T. 01625545719 F. 01625 524510 [www.ico.org.uk](http://www.ico.org.uk)

---

**From:** Merrett Rachel (NHS ENGLAND) [mailto:[r.merrett@nhs.net](mailto:r.merrett@nhs.net)]  
**Sent:** 15 October 2013 16:29  
**To:** Dawn Monaghan  
**Cc:** Roberts Siobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Greg Jones; Jonathan Bamford  
**Subject:** Re: Embargoed Press release - CONFIDENTIAL  
**Importance:** High

Hi Dawn

Yes the press were given information at noon but everything is embargoed until 0001 tomorrow. We have just received your response which is very helpful – thank you!

Best wishes  
Rachel

Rachel Merrett  
NHS England  


---

**From:** Dawn Monaghan <[Dawn.Monaghan@ico.gsi.gov.uk](mailto:Dawn.Monaghan@ico.gsi.gov.uk)>  
**Date:** Tuesday, 15 October 2013 16:14  
**To:** Rachel Merrett <[r.merrett@nhs.net](mailto:r.merrett@nhs.net)>  
**Cc:** "Roberts Siobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE)" <[siobhan.roberts@hscic.gov.uk](mailto:siobhan.roberts@hscic.gov.uk)>, Greg Jones <[Greg.Jones@ico.org.uk](mailto:Greg.Jones@ico.org.uk)>, Jonathan Bamford <[Jonathan.Bamford@ico.org.uk](mailto:Jonathan.Bamford@ico.org.uk)>  
**Subject:** RE: Embargoed Press release - CONFIDENTIAL

Hi Rachel

Our press office have had requests from the media for us to comment upon the new plans which they said were to be announced to them today at 12 noon. We have prepared a written response which our press office are going to send to your press office and copy to you.

Did you do the press meeting today or is it embargoed until tomorrow?

Regards  
Dawn

---

**From:** Merrett Rachel (NHS ENGLAND) [mailto:r.merrett@nhs.net]  
**Sent:** 15 October 2013 16:09  
**To:** Dawn Monaghan  
**Cc:** Roberts Siobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE)  
**Subject:** FW: Embargoed Press release - CONFIDENTIAL  
**Importance:** High

Hi Dawn

Please see below for info, I'll respond to your email shortly. Thanks for looking at the GP guidance. We'll hopefully send this out tomorrow.

Speak soon  
Rachel

---

**From:** Media NHSEngland (NHS ENGLAND)  
**Sent:** 15 October 2013 13:33  
**Subject:** NHS ENGLAND SETS OUT THE NEXT STEPS OF PUBLIC AWARENESS ABOUT CARE.DATA

**EMBARGOED UNTIL 00:01 WEDNESDAY 16 OCTOBER**

## **NHS ENGLAND SETS OUT THE NEXT STEPS OF PUBLIC AWARENESS ABOUT CARE.DATA**

NHS England and the Health and Social Care Information Centre (HSCIC) today set out the next steps to raise public awareness about care.data - a programme that will use information to improve the safety and care of patients.

NHS England, together with the Health and Social Care Information Centre, announced that throughout January, all 22 million households in England will receive a leaflet explaining how the new system will work and the benefits it will bring. The leaflet drop is the next stage of NHS England's public awareness plan and follows wide consultation with a range of stakeholders including GPs and patient groups. The leaflet will cost about eight pence per household, or around £1 million in total, and will clearly set out how peoples' information will be used and their right to object if they have concerns.

The NHS treats about one million people every 36 hours, collecting a vast amount of information about how patients have been treated and what their outcomes have been. At the moment, this information is held separately across the NHS.

For the first time, the care.data programme will link information from different NHS providers to give healthcare commissioners a more complete picture of how safe local services are, and how well they treat and care for patients across community, GP and hospital settings.

The information can also be used by NHS organisations to plan and design services better, using the best available evidence of which treatments and services have the greatest impact on improving patients' health.

**Tim Kelsey, NHS England's Director of Patients and Information, said:**

"I believe the NHS will make major advances in quality and patient safety through the use of this data. At the moment, the NHS often doesn't have the complete picture as information lies in different parts of the health services and isn't joined up. This programme will give NHS commissioners a more complete picture of the safety and quality of services in their local area which will lead to improvements to patient outcomes.



"To do this, we will need to link data. The HSCIC has been handling hospital data securely in this way for decades. The system is designed to be extremely secure, with a suite of safeguards to protect confidentiality. But we know not everyone will feel comfortable and we want to make sure they know they have the right to say 'no'. Patient confidentiality is non-negotiable."

The HSCIC, as the designated 'safe haven', will extract data routinely from all GP practices as well as hospitals. The data will be brought together in using automated systems in the secure environment of the HSCIC. After being linked together, the information is made available in a form that is stripped of information that could identify patients.

**Kingsley Manning, Chair of the Health and Social Care Information Centre, said:**

"The duty on the HSCIC to preserve and protect confidentiality and privacy is clear and we are determined to uphold it. The huge benefits offered by the development of care.data are also clear but can only be delivered in the context of public understanding and trust.

"Valuable feedback from doctors and members of the public has led us to decide to take this more slowly, in order to support GPs in discussing this with patients and to ensure the public in general is aware. We cannot achieve this transformation in enhanced knowledge of the effectiveness of health treatments without public support and understanding."

Everyone making healthcare decisions needs access to high quality information: clinicians need it to inform their decision making; patients need it when deciding which treatment option is best for them; and commissioners need it when making decisions about which services are right for their populations.

**Professor Peter Johnson, Cancer Research UK's chief clinician, said:**

"Using patients' data for cancer research can save lives. Analysing NHS records will help us to understand the causes of cancer, including how to prevent the disease, how we can get people diagnosed and treated faster, and what happens to people who take part in our clinical trials.

"Of course it is vital that everyone understands how their data might be used and we must make sure that there are rigorous safeguards in place to keep patients' data stored securely and used appropriately. Under these plans, people will know they still have the choice to object if they do not want their medical data being shared for research purposes."

**ENDS**

**Notes to editors**

1. For further information, please contact the NHS England press office on [nhsengland.media@nhs.net](mailto:nhsengland.media@nhs.net) or call 07768 901 293
2. The HSCIC supports better care, better services and better outcomes for patients and service users through secure data analysis and the wider provision of information. As England's legally recognised safe haven for secure data analysis, the HSCIC is focused on developing public awareness, understanding and trust in how information is used to improve care. As defined by the Health and Social Care Act 2012, the HSCIC's statutory obligations include data collection as directed by the Secretary of State and bodies like NHS England. Due consideration is given to all such requests by the HSCIC board, who by law may consult and seek appropriate guidance to ensure decisions are effectively informed. The significance of this statutory role is acknowledged in the Caldicott review "Information: to share or not to share". The HSCIC also has a substantive role in providing commissioners with the information they need to gain a clear understanding of activity and to improve the quality of services they commission for patients and service users. In addition it publishes more than 170 statistical reports a year containing anonymised data about key areas of health and social care, from public health issues to the NHS workforce and hospital activity.
3. GP guidance from NHS England, BMA and RCGP, along with supporting material can be found on care.data section of the NHS England website at: <http://www.england.nhs.uk/ourwork/tsd/care-data/>

4. A copy of the Health and Social Care Information guide to confidentiality can be found at <http://www.hscic.gov.uk/confguideorg>
5. The first extractions of data from GP practices will take place after the national awareness campaign is complete, expected to be spring 2014. Any patients who feel uncomfortable about this use of their data can object by talking to their GP practice.
6. NHS England and the HSCIC continue to work together with a wide range of stakeholders including the British Heart Foundation, Asthma UK, Arthritis Research UK, Cancer Research and Association of Medical Research Charities. Comments from our stakeholders include:

**Dr Paul Cundy, Chair of the BMA's GP IT subcommittee:** "The BMA is extremely pleased that NHS England have announced a major national awareness campaign designed to raise awareness about changes to the way that patient data is handled. It is vital that we ensure the public is fully aware about these proposals."

**Professor Peter Weissberg, Medical Director for the British Heart Foundation:** "Our medical records contain critical information that can improve the quality of care heart patients receive and help medical scientists make life-saving discoveries. With the right safeguards in place to protect patient confidentiality, this initiative will be of enormous benefit to patients and will help reduce heart disease in future."

"The British Heart Foundation believes it's in the patients' best interests to participate and we support NHS England's plans to inform the public of the benefits access to patient records can bring so that everyone can make an informed choice about participating."

**Leanne Reynolds, Research Operations Manager for Asthma UK:** "As a patient charity Asthma UK strives to make positive changes for people with asthma. But in order to make these changes we need to identify what works and what doesn't, both locally and nationally. It's really important that members of the public are aware of this programme so that they understand the benefits and can make an informed decision as to whether they want to share their data and support our research."

.....  
 .....

This message may contain confidential information. If you are not the intended recipient please inform the sender that you have received the message in error before deleting it. Please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents; to do so is strictly prohibited and may be unlawful.

Thank you for your co-operation.

NHSmall is the secure email and directory service available for all NHS staff in England and Scotland  
 NHSmall is approved for exchanging patient data and other sensitive information with NHSmall and GSi recipients  
 NHSmall provides an email address for your career in the NHS and can be accessed anywhere

.....  
 .....

.....  
 .....

This message may contain confidential information. If you are not the intended recipient please inform the

sender that you have received the message in error before deleting it.  
Please do not disclose, copy or distribute information in this e-mail or take any  
action in reliance on its contents:  
to do so is strictly prohibited and may be unlawful.

Thank you for your co-operation.

NHSEmail is the secure email and directory service available for all NHS staff in  
England and Scotland  
NHSEmail is approved for exchanging patient data and other sensitive information with  
NHSEmail and GSI recipients  
NHSEmail provides an email address for your career in the NHS and can be accessed  
anywhere

.....  
.....



Iman Elmehdawy

---

**From:** Dawn Monaghan  
**Sent:** 04 February 2014 11:33  
**To:** Jacob Smith  
**Subject:** Email chain between Geraint Lewis NHS England and Dawn Monaghan on Care data objection process 20140203

**Importance:** High

For meridio

**Dawn Monaghan**      **Group Manager, Public Services**

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.  
T. 01625545719 F. 01625 524510 [www.ico.org.uk](http://www.ico.org.uk)

---

**From:** Dawn Monaghan  
**Sent:** 03 February 2014 09:00  
**To:** 'Lewis Geraint (NHS ENGLAND)'; Merrett Rachel (NHS ENGLAND); Foster Dawn (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Wild Richard (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Roodhouse Eve (HEALTH AND SOCIAL CARE INFORMATION CENTRE)  
**Subject:** RE: Objection process Care.data  
**Importance:** High

Hi  
I'm afraid I don't have specific details I confess to not being fully across the technicalities of what is included in a record. It appeared that what was being suggested was that within the information being taken there may be other unique numbers/codes used as ID's by the NHS which like an NHS no wouldn't ID me to any individual but may ID me to those who work with those codes! I'll go back and ask the question to see if I can get a better understanding and perhaps we can discuss it on the 12<sup>th</sup>.

Too be honest; I think if there is clarity about what is contained within a medical record, what will be taken and what will not that will resolve the situation.

Many thanks  
Dawn

**Dawn Monaghan**      **Group Manager, Public Services**

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.  
T. 01625545719 F. 01625 524510 [www.ico.org.uk](http://www.ico.org.uk)

---

**From:** Lewis Geraint (NHS ENGLAND) [<mailto:geraint.lewis@nhs.net>]  
**Sent:** 31 January 2014 15:15  
**To:** Dawn Monaghan; Merrett Rachel (NHS ENGLAND); Foster Dawn (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Wild Richard (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Roodhouse Eve (HEALTH AND SOCIAL CARE INFORMATION CENTRE)  
**Subject:** Re: Objection process Care.data  
**Importance:** High

Thanks Dawn. I'm cc'ing Eve so you have her email address.

Rachel and others from my team will be very happy to help our HSCIC colleagues and then have it posted on the NHS England and NHS Choices websites.

With regard to your final paragraph, do you have more details please about what they think are these extra identifiers might be? It is important to stress that the only information being extracted from GP practices is

- (a) the four identifiers you mention (not names, for example, which are held in the data but are not being extracted)
- (b) the set of Read codes we published [here](#)

Maybe the people contacting you are (wrongly) thinking that the HSCIC is extracting free text. Free text might indeed contain identifying information but it isn't being extracted.

Any more specifics about their concerns would be helpful.

Best wishes,

Geraint

cc: Dawn Monaghan <Dawn.Monaghan@icn.nhs.uk>

cc: Rachel Merrett <r.merrett@nhs.net>

cc: Eve <eve@nhs.uk>

cc: Geraint Lewis <geraint.lewis@nhs.net> @GeraintLewis  
cc: Sam Hobson <sam.hobson@nhs.net> | +44 (0)113 2751226

cc: [NHS.uk](#) - high quality care for all, now and for future generations

---

From: Dawn Monaghan <Dawn.Monaghan@icn.nhs.uk>

Date: Friday, 31 January 2014 14:30

To: "Merrett Rachel (NHS ENGLAND)" <r.merrett@nhs.net>, "Foster Dawn (HEALTH AND SOCIAL CARE INFORMATION CENTRE)" <dawn.foster@hscic.gov.uk>, "Wild Richard (HEALTH AND SOCIAL CARE INFORMATION CENTRE)" <richard.wild@hscic.gov.uk>, Geraint Lewis <geraint.lewis@nhs.net>

Subject: Objection process Care.data

Dear all

I have a small list of things to explore at our meeting on the 12<sup>th</sup> Feb however in the meantime we have an important concern linked to feedback we are receiving in relation to the objection process and I it can't really wait until the 12<sup>th</sup> to be discussed.

I did mention this issue in my regular meeting with the HSCIC earlier in the week but since then we have several other high profile enquires regarding the issue. (Dawn I'm sorry I couldn't copy Eve into the communication as I don't have her e mail address)

The issue:

Lack of transparency to patients in relation to the 'actual' information which will be extracted from medical records for the purposes of the Care.data programme.

Although the leaflet explains in the broadest terms what will be extracted we feel there may be an expectation that if you 'object' to your data leaving the GP surgery or leaving the HSCIC then no information will be taken from your medical record. We understand this may not be the case and that information minus PCD would flow.



We would suggest that to ensure fairness and help patients fully understand the objection processes; information should be made available which clearly states what objections are available and what information will and will not be taken in the following scenarios;

1. When a patient raises no objection
2. When a patient objects to the disclosure of PDC from GP practices to the HSCIC
3. When a patients objects to PCD leaving the HSCIC

More importantly concerns have been raised with us that there are identifiers within the information kept in a medical record other than the usual ones such as name, DoB, post code and NHS no. Can you confirm with us your understanding regarding this matter?

In order to be fair it is important to be transparent about the care.data objection process.

In essence the responsibility for this transparency lies with several data controllers but it would seem sensible to us the HSCIC take the lead as they will be obliged to provide this information once they have received it.

Your prompt response would be appreciated.

Regards  
Dawn

Dawn Monaghan      Group Manager, Public Services

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.  
T. 01625545719 F. 01625 524510 [www.ico.org.uk](http://www.ico.org.uk)

.....  
.....

This message may contain confidential information. If you are not the intended recipient please inform the sender that you have received the message in error before deleting it. Please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents; to do so is strictly prohibited and may be unlawful.

Thank you for your co-operation.

NHSEmail is the secure email and directory service available for all NHS staff in England and Scotland  
NHSEmail is approved for exchanging patient data and other sensitive information with NHSEmail and GSi recipients  
NHSEmail provides an email address for your career in the NHS and can be accessed anywhere

.....  
.....







Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF  
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Karen Thomson  
Strategic Information Governance Lead  
Patients and Information Directorate  
NHS England

19 November 2013

Clare Sanderson  
Director of Information Assurance  
The Health and Social Care Information Centre

Dear Karen, Clare

This letter offers our view on whether the NHS Commissioning Board (NHSCB) and the Health and Social Care Information Centre (HSCIC) are data controllers solely, jointly or data processors in relation to the data obtained by the HSCIC under direction of NHSCB from health bodies for the first stage of Care.data.

The NHSCB clearly determines the purpose for information which it directs the HSCIC to obtain and process and therefore the NHSCB is a data controller. Given that the HSCIC has a considerable degree of independence as to how it is to carry out its processing functions and the HSCIC is exercising a statutory function in processing personal data, it does not appear likely that the HSCIC is merely a data processor in relation to the personal data it handles and is therefore a joint data controller with NHSCB.

We have based our approach on our reading of the Health and Social Care Act 2012 which has informed our view as to the DPA responsibilities of these bodies. We appreciate that there is a considerable amount of new legislation in this area and we would want our analysis to be based on the fullest understanding of the provisions affecting the bodies within the new NHS structure. If you believe we have misunderstood any of the legislative provisions in the HSCA 2012 or if there is further legislation affecting our findings of which we should be aware, we should be most grateful for your assistance in directing us to the relevant provisions.

#### **Information obtained by HSCIC**

Whilst the HSCIC is to collect information on instruction (direction) from the NHSCB, once it has obtained the data it is to have considerable freedom in

how it records and uses the data (per The Health and Social Care Act 2012 (HSCA) Section 255, 257, 258 and 261).

It would appear that the HSCIC determines the manner in which, and to a certain extent the purpose for which, personal data is processed. The Secretary of State or NHSCB must consult with the HSCIC before making a direction. Input from the HSCIC (presumably as to how data is to be collected and managed is therefore required before the direction is given). The HSCIC therefore contributes to determining the manner and the purpose for which personal data is processed and is therefore a data controller in respect of such data. In addition, section 1(4) DPA provides that, where an organisation processes personal data only for purposes for which they are required by or under any enactment to be processed, the organisation is the data controller of such data.

#### **When a third party determines the purpose of processing**

Where a third party determines the purpose for which the data is to be processed, for example, as the NHSCB may, but the HSCIC determines the manner in which the processing to take place, the HSCIC and the third party are likely to be joint data controllers in respect of the relevant data.

It is our view that this will be the case in respect of the data to be obtained by the HSCIC from general practitioners in response to the proposed direction from the NHSCB.

Although a third party (either the NHSCB in making a direction or another party making a request) may determine the broad purpose for which the HSCIC is to process the data, the disclosure of such data by the HSCIC to the third party is to be 'treated as a dissemination of that information to that person'. Applying our above view that the NHSCB and HSCIC would be joint data controllers, it may appear odd to describe sharing between them as a 'dissemination', which implies a disclosure to a wider group.

However, we are reading this provision as simply a means of ensuring that all the requirements for the dissemination of data by the HSCIC are followed, even where the dissemination is to the party that directed/requested the processing in the first place.

Therefore, on this interpretation, the provision does not affect the determination of the roles of the parties in relation to the data for the purposes of the DPA as joint data controllers.

### **How further processing affects data controller status**

Where the HSCIC 'disseminates' the information it has obtained and processed in accordance with the first direction to the NHSCB, if the NHSCB then processes the returned data for its own purposes it will be the sole data controller in respect of the returned data. The HSCIC will however continue to be a joint data controller with the NHSCB in respect of any copy of such data it continues to process in accordance with the original NHSCB direction to obtain and process the data.

### **In the context of performing a statutory function**

Where the NHSCB carries out, or instructs others (e.g. the HSCIC) to carry out on its behalf, any processing of personal data in connection with the exercise of its statutory functions, the NHSCB will be the data controller in respect of the data being processed.

The HSCIC also has statutory functions involving the processing of personal data. The HSCIC will process personal data in accordance with its statutory obligation to establish and operate information management systems.

The HSCIC will also process personal data in accordance with its statutory obligation to comply with directions made by the NHSCB. The HSCIC will therefore also be a data controller in respect of the personal data which it is obliged by statute to process. The NHSCB and the HSCIC will be joint data controllers in respect of the personal data processed by the HSCIC in response to the direction by the NHSCB.

### **If the HSCIC process data at the request of a party other than NHSCB**

Where, in accordance with a statutory obligation, the HSCIC processes personal data at the request of a third party other than the NHSCB, the HSCIC may be a joint data controller with that party (rather than the NHSCB) in respect of the data processed in response to the request.

### **Practical implications of joint data controller status**

Where two bodies are joint data controllers, they are both liable for compliance with the data protection principles. However, they may, where appropriate, agree between themselves which party is to satisfy which of the data protection obligations of a data controller in connection with the processed data.

Responsibility for compliance with data protection obligations should be determined between the joint data controllers in accordance with their respective functions. For example, issues of unfairly obtaining or unlawfully processing could be the responsibility of the NHSCB who will have determined the purposes for which the data is obtained and processed, whilst responsibility for the security of data and for handling subject access requests could fall to the HSCIC who has physical control of the data.

Such arrangements should reflect the reality of the relationship between the parties (e.g. who physically holds the data and who has the appropriate expertise or resources to satisfy data protection obligations) and should provide clarity as to respective responsibilities for both the joint data controllers and data subjects. When these practicalities are decided, it may be appropriate to include reference to such responsibilities in any memorandum of understanding between NHSCB and the HSCIC.

We hope you find this letter has adequately explained our view on this matter.

Yours sincerely

**Dawn Monaghan**  
**Group Manager, Public Services**



Leaflet  
design  
approval

National media -  
programme update to  
include announcement of  
further national awareness

in file  
approval

HSCIC  
contract  
award

Preparation for  
care data concept info  
film (estimate - 4 wks)

Provide Patient Information Line (3 months)

Printing  
(est. 4 wks)

Leaflet  
distribution to  
households  
(over 4 wks)

Fair processing period of awareness local regional and national programmes  
Over a period of 6 months

Data sharing information packs  
mailed to all GP practices in  
England

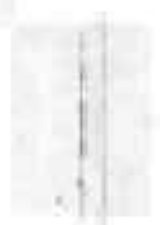
1<sup>st</sup> extract  
linkage &  
analysis

2<sup>nd</sup> extract  
linkage &  
analysis

3<sup>rd</sup> extract  
linkage &  
analysis

Apply lessons from  
pilot

Service  
go-live



Iman Elmehdawy

---

From: Dawn Monaghan  
Sent: 04 February 2014 11:28  
To: Jacob Smith  
Subject: NHS England and ICO Meeting on Care.Data info - 20131205  
Attachments: 4.11.13 NHSE Care dataPIAv0.7.docx; Agenda - Care Data Meeting NHS England and ICO 5 December RM.docx; Care data Data Controliership letter191113.pdf; Minutes - Care Data ICO meeting 19 September 2013 draft final.docx

For meridio

Dawn Monaghan      Group Manager, Public Services

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.  
T. 01625545719 F. 01625 524510 [www.ico.org.uk](http://www.ico.org.uk)

---

From: [REDACTED] (NHS ENGLAND) [mailto:[REDACTED]@nhs.net]  
Sent: 28 November 2013 16:55  
To: Roberts Siobhan (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Outram Christine (NHS ENGLAND); Lewis Geraint (NHS ENGLAND); Flynn Peter (NHS ENGLAND); Merrett Rachel (NHS ENGLAND); Thomson Karen (NHS ENGLAND); Dawn Monaghan; David Evans; Jacob Smith; Victoria Cetinkaya; sanderson clare (HEALTH AND SOCIAL CARE INFORMATION CENTRE); Dawn Monaghan; Roodhouse Eve (HEALTH AND SOCIAL CARE INFORMATION CENTRE)  
Cc: David Evans  
Subject: NHS England and ICO Meeting on Care.Data

Dear all

Please find the following documents attached for the meeting scheduled Thursday, 5<sup>th</sup> December 2013:

- i. Agenda
- ii. Minutes from meeting held 19<sup>th</sup> September 2013
- iii. PIA
- iv. Data Controliership letter

I hope you find this all in good order.

Regards

[REDACTED]  
Strategic Intelligence  
Care.Data - Patients & Information

NHS England  
2575 Quarry House | Quarry Hill | Leeds | LS2 7UE

[REDACTED]  
[nhs.net](http://nhs.net)  
[www.nhs.uk](http://www.nhs.uk)

NHS England: High quality care for all, now and for future generations



This message may contain confidential information. If you are not the intended recipient please inform the sender that you have received the message in error before deleting it. Please do not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents; to do so is strictly prohibited and may be unlawful.

Thank you for your co-operation.

NHSmail is the secure email and directory service available for all NHS staff in England and Scotland  
NHSmail is approved for exchanging patient data and other sensitive information with NHSmail and GSI recipients  
NHSmail provides an email address for your career in the NHS and can be accessed anywhere

# Privacy impact assessment:

## Care.Data Programme

### Version 0.7

### November 2013

1	Executive Summary .....	2
2	The purpose of a privacy impact assessment .....	3
3	What is care.data?.....	3
4	Privacy issues as a consequence of care.data .....	5
4.1	The extraction of personal confidential data into the HSCIC .....	6
4.2	The processing of the personal confidential data when held by the HSCIC.....	8
4.3	The onward of disclosure of data from the HSCIC .....	11
4.4	Conclusion of privacy issues as a consequence of care.data .....	13
5	Business case .....	14
6	Alternatives to identifiable data .....	17
7	What will we do to protect privacy? .....	18
7.1	Information Governance Controls .....	18
7.2	Additional care.data pledges to protect information.....	19
8	Public Acceptability .....	20
8.1	Independent scrutiny.....	20
8.2	Patient Information Materials.....	20
9	Conclusions.....	21
10	Appendices .....	23
	Appendix A - Managing Privacy Risk.....	23
	Appendix B – Examples of use .....	25
	Appendix C – Definition of Terms.....	27

NHS England (formerly the NHS Commissioning Board [NHS CB]<sup>1</sup>) was established on 1 October 2012 as an Executive Non-Departmental Body.

NHS England aims to ensure high quality care for all, now and for future generations. We are committed to transparency and to putting patients and the public at the heart of all decisions, grounded by the values and principles of the NHS Constitution. The responsibilities of NHS England can be divided into the following domains:

- Reducing mortality
- Improving care for patients with long term conditions
- Improving acute care
- Improving patient experience
- Improving patient safety

Care.data will bring together securely, health and social care information from all care settings in order to improve the quality, efficiency, and equity of services. For the first time, it will allow nationwide linkage of primary and secondary care data in order to identify any unwarranted variations in care across the country. Care.data will enable increased use of information that the NHS already collects with the intention of improving healthcare, by ensuring that timely and accurate data are made available to NHS commissioners, providers, and researchers.

Under the Health and Social Care Act 2012, NHS England can direct the Health and Social Care Information Centre (HSCIC) to collect data from every provider of care funded by the NHS. This is limited to where the data are necessary for exercising the functions of NHS England. These data are collated, stored, and disseminated or published by the HSCIC rather than NHS England. The HSCIC provides a secure data environment, which operates to the very highest technical and security standards. The HSCIC will disseminate data in three formats:

- 1) Anonymous or aggregated data will be published in line with Information Commissioner's Office (ICO) anonymisation code of practice, e.g. with small number suppression, to ensure that the risk of re-identification is very remote<sup>2</sup>.
- 2) Pseudonymised<sup>3</sup> data will be made available to specific approved groups of users, initially for commissioning uses only and in line with ICO guidance (see section 4.3 Figure 2)
- 3) Identifiable data will only be made available where there is a legal basis for doing so (e.g. with patient consent or approval under section 251 of the NHS Act 2006).

A privacy impact assessment (PIA) is a tool, process or method to identify, assess, mitigate or avoid privacy risks. This PIA describes how data will be collected, processed, disseminated and published for care.data. It explains what the programme will do to protect

<sup>1</sup> NHS England is the operating name of the NHS Commissioning Board as established by the Health and Social Care Act 2012. It is referred to throughout this document as NHS England.

<sup>2</sup> Anonymisation: managing data protection risk code of practice  
[http://www.ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/anonymisation](http://www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation)

<sup>3</sup> The process of distinguishing individuals in a dataset by using a unique identifier, which does not reveal their 'real world' identity.

privacy and the solutions that have been identified and implemented to help safeguard privacy. This document will enable readers to assess for themselves what may be considered a potential impact on their privacy.

The HSCIC has undertaken a PIA for all the personal data it processes, which includes the data extracted for care.data.<sup>4</sup> The HSCIC provides many of the technical and information governance controls for care.data therefore this PIA draws upon the overarching HSCIC PIA. This PIA, however, specifically considers the privacy impact of care.data in greater detail.

## 2 The purpose of a privacy impact assessment

Privacy impact assessments (PIAs) were launched in the UK by the Information Commissioner in December 2007 and were mandated by the Cabinet Office for information and communications technology (ICT) projects following the Data Handling Review of June 2008<sup>5</sup>.

The Health and Social Care Act 2012 introduces legislative powers that enable NHS England to direct the HSCIC to obtain and process identifiable patient data in certain circumstances without the need for patient consent. This arrangement includes care.data.

Patients, and those people legally empowered to act on their behalf, must be informed about how identifiable data about them are used. Therefore, alongside other awareness-raising activities, NHS England and the HSCIC are informing patients about how care.data might affect the privacy of personal data. The privacy impact assessment:

- Describes the purpose and objectives of the care.data programme;
- Assesses the potential implications for privacy; and
- Explains what NHS England and the HSCIC will do to protect privacy.

The scope of this PIA will cover the whole of the care.data programme, including each of the domains of health and social care information that are currently planned to be included within the programme. The care.data programme has a number of phases relating both to the data sets to be acquired and the functionality offered. All of these phases will be encompassed by this PIA. The first phase is the linkage of GP data with hospital data so the emphasis, in this first iteration, is on this element. The PIA will be kept under review and revised as the detail for each phase is developed. We welcome feedback on this PIA.

## 3 What is care.data?

The care.data programme is a major upgrade of the Hospital Episodes Statistics (HES) service that will link a more complete range of data at record level across England. It will collect, collate and link clinical and other data from all health and care settings, including hospital, primary care, community, mental health and social care. The combined datasets will be made available to others in a range of formats, with all appropriate safeguards in place to protect confidentiality.

<sup>4</sup> [http://www.hscic.gov.uk/media/12931/Privacy-Impact-Assessment/pdf/privacy\\_impact\\_assessment\\_2013.pdf](http://www.hscic.gov.uk/media/12931/Privacy-Impact-Assessment/pdf/privacy_impact_assessment_2013.pdf)

<sup>5</sup> [http://www.ico.org.uk/about\\_ico/consultations/~/media/documents/library/Corporate/Research\\_and\\_reports/pia-executive-summary.pdf](http://www.ico.org.uk/about_ico/consultations/~/media/documents/library/Corporate/Research_and_reports/pia-executive-summary.pdf)

Specifically, the programme's purposes are:

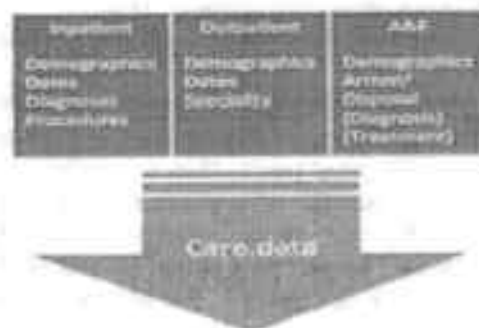
- i. Greater accountability
- ii. Informed choice
- iii. Greater efficiency
- iv. Better outcomes
- v. Customer services
- vi. Economic growth

Currently, health and social care data are not joined together in order to provide a complete view of the patient journey. This makes it difficult or impossible to assess the safety, effectiveness and efficiency of health and care services. To address these shortcomings, care.data will collect and link data from different health and social care settings.

For many years, data have been collected from all hospitals providing NHS care. This dataset, HES, has been used for tens of thousands of research studies and clinical audits. However, by definition, HES is limited to hospital data whereas the bulk of NHS care episodes occur in community settings. As a result, commissioners are often unable to ensure that joined-up care is being provided to their patients.

The care.data programme is designed to ensure that commissioners have access to a dataset that contains linked information from all GP practices and all hospitals. Over the following years, data will be progressively added from all other care settings, including community health services and social care, and the hospital dataset itself will become much richer and more complete. This transformation will see Hospital Episode Statistics (HES) evolve into a care episode service (CES).

## From HES



## To CES

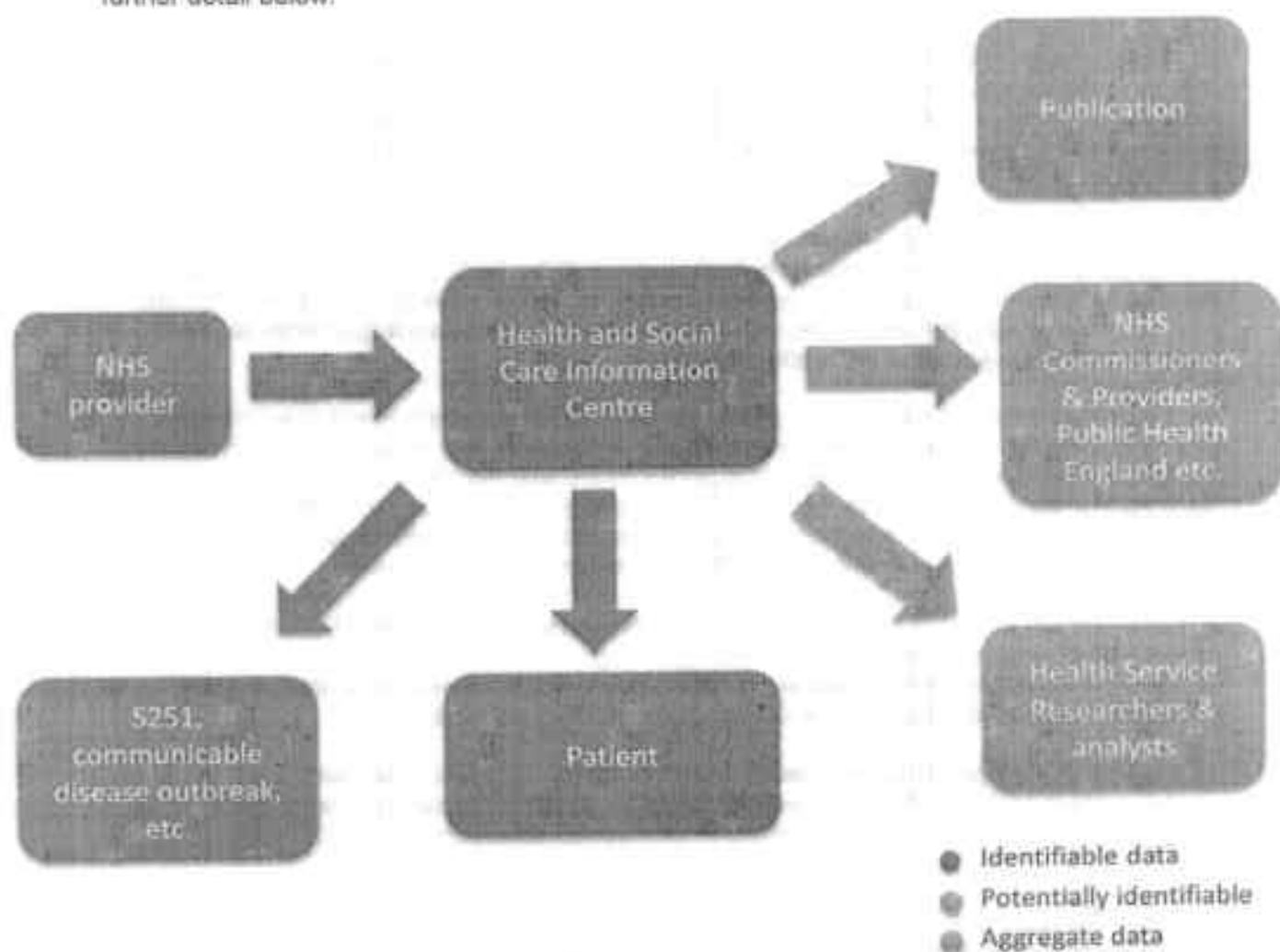


The HSCIC will collect and process the data for care.data using its powers under the Health and Social Care Act 2012. The HSCIC is England's central, authoritative source of health and social care information. The HSCIC will process patients' confidential data in a secure environment and will only release confidential data where there is a legal basis for doing so.

The main functions of the HSCIC in relation to care data are to:

- i. collect and process, patient identifiable data extracted from patient records;
- ii. assure the data quality of patient identifiable data;
- iii. link and de-identify patient identifiable data;
- iv. publish aggregate data;
- v. disseminate potentially identifiable data to approved bodies and where strict controls exist so the likelihood of an individual being identified are very small;
- vi. disseminate patients and specific bodies patient identifiable data (only where necessary, in exceptional circumstances and when lawfully authorised e.g. under section 251 of the NHS Act 2006). This is a future aim and subject to independent approval.

The following diagram shows how the linked dataset will be made available in order to realise the benefits outlined above. The privacy impact of these data flows is considered in further detail below.



#### 4 Privacy issues as a consequence of care data

This section assesses the potential impact on privacy of care data. To assess the potential privacy impact of care data, it is necessary to weigh up not only whether the impact is positive, neutral or negative but also to consider the extent to which any adverse impact on



privacy may be acceptable if it brings other benefits. Safeguards to protect privacy are explained in section 8 - What will we do to protect privacy?

Care.data involves the extract of personal confidential data from health records, including *sensitive personal data* as defined in the Data Protection Act 1998. Identifiers (NHS number, date of birth, postcode and gender) are extracted from providers together with coded clinical information and sent to the HSCIC. As with any disclosure of personal confidential data, there are associated risks to privacy and confidentiality.

The privacy impact can be considered in three areas:

- The extraction of personal confidential data into the HSCIC
- The processing of the personal confidential data when held by the HSCIC
- The onward of disclosure of data from the HSCIC

#### **4.1 The extraction of personal confidential data into the HSCIC**

---

The Health and Social Care Act 2012 provides a legal basis for the extraction of personal confidential data in certain circumstances. The Act sets aside the requirement under the common law duty of confidence to seek patient consent<sup>6</sup>. Certain requirements under the Data Protection Act 1998 continue to apply – in particular, the fair processing principle, which means that patients must be made aware of how confidential data are processed for care.data.

The extraction of personal confidential data from providers without consent carries the risk that patients may lose trust in the confidential nature of the health service. This risk is two fold: firstly, patients will not receive optimal healthcare if they withhold information from the clinicians that are treating them; and secondly, that this loss of trust degrade the quality of data for care.data and other secondary uses of NHS data.

To mitigate against the risk, NHS England has committed to giving patients the right to object to personal confidential data leaving their GP practice and, other than in exceptional circumstances, to having their objections upheld in line with the commitment given by the Secretary of State for Health in April 2013<sup>7</sup>. Previously there was no straight forward mechanism for patients to exercise this right. This is therefore a step forward in enabling patients greater control over the identifiable information held about them.

It is important to note that personal confidential data have been processed for many years where there has been a legal basis for doing so (e.g., where there has been special approval for medical purposes such as research). This new objection extends to all disclosures of personal confidential data from the GP practice, not just care.data.

At present, it is not possible for patients to prevent flows of confidential data from other care settings into the HSCIC, for example from hospitals. For this reason, we have ensured that patients can also object to the disclosure of confidential data from the HSCIC (see section 4.3).

In order to ensure that patients are aware of the changes to how data are processed for care.data, and to ensure they are aware they can object, a number of awareness raising activities will be undertaken. Figure 1 summarises the awareness raising activities that are taking place.

---

<sup>6</sup> Under Sections 259 and 256 of the Health and Social Care Act 2012

<sup>7</sup> At the launch of the Caldicott Information Governance Review Report 26 April 2013

### Figure 1 - Summary of supporting activities and resources

1. A patient leaflet and poster about information sharing made available in GP practices
2. Materials developed in accessible formats including Braille, large print and audit versions.
3. Materials for GP practices to support patient awareness raising including a how to guide and a template press release for local tailoring
4. Detailed FAQs for both GPs and patients
5. Testing of these materials in a limited number of GP practices with feedback incorporated into the national version of the leaflet and poster.
6. A mailing of a leaflet about information sharing to every household in England
7. Separate GP and patient information lines to support understanding
8. Regional events for GPs and NHS managers to encourage awareness raising at a regional level for example via regional press releases.
9. Social and digital media: dedicated web support pages for patients through NHS Choices and for professionals through NHS England.
10. Use of central social media channels to help raise awareness and to direct to particular FAQs such as objection process.
11. Engagement with a number of national patient groups, charity and voluntary sector organisations to enable cascade of messages through their regular and social media channels.

In order to evaluate the potential impact on their privacy, patients need to understand what data are to be extracted. As explained above in section three, the first stage of CES will involve linking GP data to hospital data. Data from other parts of the health and social care service will be linked over time and this PIA will be updated to reflect this. The dataset extracted from GP systems has been published<sup>8</sup> and includes data such as referrals, prescriptions, symptoms, diagnoses, and treatments. Whilst all health data is classified as sensitive personal data under the DPA, a list of particularly sensitive items will be excluded from extracts<sup>9</sup>. The data extracted is in the format of a series of codes. Free text (i.e., words, sentences, and paragraphs) will not be extracted for care data.

Extraction of the GP data will be on a monthly basis using the General Practice Extraction Service (GPES). This is a tool provided by the HSCIC, which extracts data from GP practices into the HSCIC. Data recorded in GP records from Autumn 2013 will be extracted, in the first instance, provided that it is an item included in the published dataset. The analysis of historic data would bring much greater insight into the provision of care and opportunities for valuable research so this is the longer-term vision, however, a phased approach is being adopted.

In accordance with the Data Protection Act 1998, only the minimum necessary patient identifiable data will be collected. The GP dataset has been considered by an independent group of clinical informatics experts, which included representatives from the British Medical Association (BMA) and the Royal College of General Practitioners (RCGP). The group was satisfied that the dataset seemed appropriate for commissioning. Any future changes to the dataset or to its scope will be subject to further review by the group. In addition, the care data proposal was also reviewed and approved by the GPES Independent Advisory Group (IAG), which includes clinical and patient representation. Any changes or updates to the dataset will be published on the NHS England website.

<sup>8</sup> <http://www.england.nhs.uk/wp-content/uploads/2013/08/cd-ces-tech-spec.pdf>

Reasons for processing and benefits	Impact on privacy	Controls and Pledges
<ul style="list-style-type: none"> <li>• Data collected are fundamental to the NHS, and/or necessary to improving public health or health services.</li> <li>• Personal confidential data are extracted from healthcare providers to enable linkage.</li> </ul>	<ul style="list-style-type: none"> <li>• Some people may feel a loss of individual autonomy (no patient consent)</li> <li>• Some patients not be aware of or understand their choices.</li> </ul>	<ul style="list-style-type: none"> <li>• Statutory basis for data collection required or permitted by law<sup>9</sup></li> <li>• Identifiable data must be necessary to satisfy the purpose</li> <li>• Awareness raising activities will help patients understand how their data are used not only for care data but other uses of healthcare.</li> <li>• Patients can object to the processing of the personal confidential data in GP records.</li> <li>• Patients can change their mind at any time and identifiers can subsequently be removed from the HSCIC</li> <li>• Control 1 (see Section 7 – ‘Information Governance Controls’)</li> <li>• Pledge B, C and D (see section 7 – ‘Additional care data pledges to protect information’)</li> </ul>

#### 4.2 The processing of the personal confidential data when held by the HSCIC

Under the Health and Social Care Act 2012, the HSCIC is established as a ‘safe haven’ with powers to collect and analyse confidential information about patients. The HSCIC will process the personal confidential data for the care.data service.

The HSCIC’s PIA<sup>10</sup> details the risks and responsibilities it has to protect the confidentiality of all the data it holds. This PIA is much broader than the care.data PIA because the HSCIC is

<sup>9</sup> The Health and Social Care Act provides powers for the Health and Social Care Information Centre to require organisations to submit data to it when data collection has been mandated by NHS England or Secretary of State, and in some circumstances, where requested by other bodies.

<sup>10</sup> [http://www.hscic.gov.uk/media/12931/Privacy-Impact-Assessment/pdf/privacy\\_impact\\_assessment\\_2013.pdf](http://www.hscic.gov.uk/media/12931/Privacy-Impact-Assessment/pdf/privacy_impact_assessment_2013.pdf)

the data controller for numerous datasets in addition to those collected for the care.data programme. As stated in the HSCIC PIA, 'the HSCIC like all organisations that process and store patient identifiable data, must protect the confidentiality of that data and must guard against risks and threats from inside and outside the organisation'. The risks described include threats associated with 'cyberspace' such as hackers attempting to access the data illegally. The HSCIC PIA describes in detail how these risks and threats are addressed and minimised by effective information governance controls.

Processing of data by the HSCIC has a potential impact on privacy because the HSCIC is an organisation to which patients have not disclosed information themselves. At a local level, personal confidential health data have been used for many years for the purposes of indirect care (e.g. for planning services, audit, and research). There have been incidents of local data breaches and also a misunderstanding of the complex legal and information governance framework for health data. Local processing can be difficult to monitor and audit, and the likelihood of an individual being identifiable when processing takes place locally is higher than when data are processed centrally (e.g. recognising the name of a neighbour). Whilst a centralised data collection has potential privacy implications, these risks can be balanced with a reduction in the requirements for local processing of personal confidential data and with assurances that data processing by the HSCIC is to the highest security standards. The technical expertise and detailed knowledge of information governance is very difficult to match across all organisations operating at a local level.

It is necessary for the HSCIC to receive identifiers so that it can link data from different healthcare settings to realise the benefits outlined in section six. Data linkage involves matching together the records from two or more care settings about the same patient to provide a more complete picture of the patient's needs, experiences of care, and outcomes. For example, hospital records and general practice records could be linked in order to analyse the impact upon outcomes of different care pathways for a particular condition.

The privacy risks associated with the HSCIC are mitigated because the process of linking the record is automated. Occasionally, in a small number of cases, it is necessary for HSCIC analysts to check the data for data quality reasons. However, this human involvement is done following strict rules and processes, all of which are designed to protect the confidentiality of the individual. These include, for example, rules around retaining the data, destroying the data, disclosing the data and illegally matching data to identify individuals. Patient identifiers (NHS number, date of birth, postcode and gender) are held separately from clinical data and wherever practicable HSCIC staff are assigned access rights to either the patient identifiers or the clinical data not both.

It is important to reiterate that the data that the HSCIC processes for care.data do not include patients' names and addresses. Furthermore, the data are presented in terms of clinical codes rather than free text (i.e., no words, sentences, or paragraphs). Once the record has been linked, the identifiers are removed so a new record is created that does not identify the patient.

Where patients have objected to the flow of their personal confidential data from the general practice record, the HSCIC will receive clinical data without any identifiers attached (i.e. anonymised data).

If a patient objects to flows of personal confidential data from their GP practice and also from the HSCIC (see section 4.3) then it is necessary for the patient's NHS number to flow to the HSCIC so that the HSCIC is aware of this objection and can stop personal confidential data it holds from other care settings leaving the HSCIC. This has been described to patients in FAQs.

Reasons for processing and benefits	Impact on privacy	Controls and Pledges
<ul style="list-style-type: none"> <li>• Accuracy has to be checked before data are de-identified (it is not possible afterwards)</li> <li>• De-identification so that the data can be used more freely for the benefit of patients.</li> <li>• Information use by the public to make healthcare decisions and by people inside and outside the NHS for activities such as medical research, public health and national clinical audit, has to be good quality. The HSCIC is responsible for ensuring this.</li> <li>• Linking data from different healthcare settings is a powerful means of increasing knowledge and can bring benefits to commissioning, in medical research and public health.</li> </ul>	<ul style="list-style-type: none"> <li>• Data collection, storage and processing creates risk of confidential information being accessed without the knowledge or consent of patient.</li> <li>• Risks in terms of changes to scope (e.g. to dataset) without patients being aware.</li> </ul>	<ul style="list-style-type: none"> <li>• Statutory basis for collection and analysis.</li> <li>• Identifiable data stored only where necessary and destroyed or aggregated, anonymised or pseudonymised as soon as possible.</li> <li>• A single national extraction reduces the need for local processing of personal confidential data where patients are more likely to be identifiable or where the safeguards in place, may not be as robust.</li> <li>• Patient identifiers are held separately from clinical data within the HSCIC.</li> <li>• De-identifying data reduces or eliminates the risk of a person's identity being revealed and thus helps protect privacy</li> <li>• Approval from an Independent Advisory Group for any changes to scope, e.g. to the GP dataset, and publication of the minutes and recommendations of this group<sup>11</sup>.</li> <li>• Controls 1, 2, 3, 4 and 7 (see Section 7 – "Information Governance Controls")</li> <li>• Pledges A, B, C, D, E and F - (see section 7 – "Additional care data pledges to protect information")</li> </ul>

<sup>11</sup> The GPES Independent Advisory Group consider proposals to change the GP element of care data and information is provided at: <http://www.hscic.gov.uk/article/1858/GPES-independent-Advisory-Group>



### 4.3 The onward of disclosure of data from the HSCIC

---

The law pulls in different directions where dissemination of information is concerned; human rights legislation, data protection legislation, and the common law duty of confidentiality all require us to protect information that could identify an individual. The Health and Social Care Act 2012, however, allows the HSCIC to obtain and disseminate information about patients when acting under direction from the Secretary of State or NHS England.

The data flows diagram in section 3 shows how data will be made available from the HSCIC. There are three categories of disclosure:

- Green flow – aggregate data
- Amber flow – potentially identifiable data
- Red flow – personal confidential data

Green flows of data will be published only in aggregated form with additional safeguards (e.g., small number suppression) so the risk of identifying an individual is very remote. This will be in line with the ICO code of practice on anonymisation<sup>12</sup> and the Information Standards Board anonymisation standard for publishing health and social care data<sup>12</sup>. Transforming identifiable data into anonymised data protects personal privacy and enables published information to be used for public benefit.

Amber data will only be disclosed by the HSCIC to a finite number of approved users such as commissioners and approved researchers. Amber data are pseudonymised in line with ICO guidance.

There is a remote risk that a patient could be identified even though identifiers are removed (e.g. if you knew a patient with a rare disease lived in a particular area). However, the ICO advises that limited access allows the disclosure of richer data<sup>2</sup>. All amber disclosures will be in accordance with robust information governance controls listed in figure 2.

**Figure 2 - The following robust safeguards will be in place in relation to disclosure of data by the HSCIC:**

- purpose limitation, i.e. the data can only be used by the recipient for an agreed purpose or set of purposes;
- training of recipients' staff with access to data, especially on security and data minimisation principles;
- controls over the ability to bring other data into the environment, allowing the risk of re-identification by linkage or association to be managed;
- limitation of the use of the data to a particular project or projects;
- restriction on the disclosure of the data;
- prohibition on any attempt at re-identification and measures for the destruction of any accidentally re-identified personal data;
- arrangements for technical and organisational security, e.g., staff confidentiality agreements;
- encryption and key management to restrict access to data;
- limiting the copying of, or the number of copies of the data;
- arrangements for the destruction of the data on completion of the project; and

<sup>12</sup> <http://www.isb.nhs.uk/news-folder/anon>



- penalties, such as contractual ones that can be imposed on the recipients if they breach the conditions placed on them.

Whilst there is privacy risk that the analysts granted access to these pseudonymised flow could potentially re-identify patients maliciously by combining the pseudonymised data with other available datasets (a technique known as a jigsaw attack) such an attack would be illegal and would be subject to sanction by the ICO.

**Red Flows** – These flows involve the disclosure of personal confidential data from the HSCIC and are only permitted where there is a legal basis for example, explicit patient consent, approval under section 251 of the NHS Act 2008 or exceptionally where there is an overriding public interest in disclosure such as an outbreak of a new disease or a civil emergency. In order to establish trust in care data from patients and healthcare professionals, personal confidential data collected for care data will initially only be disclosed where there is an overriding public interest even though disclosures under section 251 or with patient consent would be legally permissible.

If it is agreed in the future<sup>13</sup> that personal confidential data, collected as part of the care data programme, will be disclosed by the HSCIC e.g. where there is section 251 approval, patients can object to this by informing their GP and such objections will be honoured. GPs can register such objections by entering a code into the GP record.

As stated in section 4.1, there is not a straight forward process for patients to prevent data flows from other care settings, e.g. hospitals, to the HSCIC. This code prevents personal confidential data derived from any healthcare setting leaving the HSCIC unless there is an overriding public interest such as a civil emergency.

Whilst it is possible for patients to object to the processing of personal confidential data under section 10 of the Data Protection Act 1998, this new code allows patients to exercise, to a large degree, choice more easily: they simply need to ask their GP to enter this code into their GP practice record. Put simply, patients who are concerned about their privacy can now control the flow of confidential data both out of their GP practices and out of the HSCIC.

Reason for processing and benefits	Impact on privacy	Controls and Pledges
<ul style="list-style-type: none"> <li>• Once data are de-identified they can be used without breaching confidentiality for a large number of "secondary purposes" that are fundamental to the operation of the NHS and/or necessary to improving public health or health and social services where jointly commissioned with the NHS.</li> </ul>	<ul style="list-style-type: none"> <li>• In some cases, a small residual risk that identifiable data could be revealed<sup>23</sup></li> <li>• Risks of jigsaw attacks increase as more effectively anonymised data are made available, to more organisations.</li> </ul>	<p><b>Green data:</b></p> <ul style="list-style-type: none"> <li>• Anonymisation techniques will be applied as described in the Appendix 2 of the ICO's anonymisation code e.g. small number suppression, rounding up or down of numbers etc.</li> </ul> <p><b>Amber data:</b></p> <ul style="list-style-type: none"> <li>• Robust information governance controls will</li> </ul>

<sup>13</sup> Changes to scope are subject to independent review.

<ul style="list-style-type: none"> <li>• Data are used to help plan and monitor services, understand the health needs of patients and improve the quality of health care provision.</li> <li>• Data are used to understand the outcomes that patients receive, as well as the patient experience and efficiency of the service.</li> <li>• Information used by the public to make health care decisions, and by people inside and outside the NHS for activities such as medical research, public health intelligence and clinical audit on a national scale.</li> <li>• Comparing the quality of care provided by different hospitals to identify outliers, using the lessons learnt from those performing exceptionally well and take urgent steps to investigate and address those organisations performing less well.</li> </ul>		<p>be applied as detailed in figure 2.</p> <p><b>Red data:</b></p> <ul style="list-style-type: none"> <li>• Disclosures of personal confidential data will be limited in the first instance to exceptional circumstances for example in the event of a civil emergency.</li> <li>• Disclosures of personal confidential data can only occur where there is a legal basis for example under section 251 of the NHS Act 2006.</li> <li>• Patients can object to their personal confidential data leaving the HSCIC.</li> <li>• Controls 5, 6, 7 (see Section 7 – "Information Governance Controls")</li> <li>• Pledges A, B, C, D and E (see section 7 – "Additional care.data pledges to protect information")</li> </ul>
--	--	--

#### 4.4 Conclusion of privacy issues as a consequence of care.data

The main tension identified within this privacy assessment is the balance between the benefits of:

- using linked personal confidential data from health and social care records to improve the quality, efficiency, and equity of care provision through better commissioning of services with a focus on safety, outcomes and patient experience; versus
- the risks to patient privacy from the collection, linkage, storage and dissemination of the data in a variety of formats.

A key component of any assessment is the degree to which these risks are mitigated by the controls and security that will be applied. In this case, only the HSCIC will process data in

identifiable form, an arrangement that markedly limits the risks to an individual that their privacy will be breached by this programme. Moreover, a potential positive impact of care data is that more organisations should be able to use pseudonymised information where they currently use identifiable information.

As also referenced in the HSCIC PIA the potential risks to privacy from care data are:

- A. Loss of individual autonomy from use of patient identifiable data without consent
- B. Risk of confidential information being accessed and viewed without knowledge or consent of patients
- C. Linking and de-identification processes may not be reliable enough to achieve total anonymisation of data
- D. Risk of data being accessed illegally and then sold or otherwise misused by commercial organisations, criminals or others; and
- E. Risk of data being accessed legally and then the data being misused.

The actual mitigating controls that the care data programme will use to safeguard these risks are summarised below with more details in section 7. The HSCIC will:

- A. Obtain and process only the minimum necessary patient identifiable data from other organisations
- B. Store and process data in its capacity as "safe haven", under the Health and Social Care Act 2012
- C. Keep to the absolute minimum the number of staff able to access and view patient identifiable data, and wherever practicable assign staff rights of access to either patient identifiers or clinical data but not both
- D. Destroy data held in identifiable form as soon as they are no longer required, or in accordance with the HSCIC's retention policy
- E. Disclose only anonymised data, unless there is a legal basis for the disclosure of confidential data.
- F. When disclosing anonymised data, restrict the data disclosed according to the context in which the data will be used.
- G. Monitor who accesses patient identifiable data.

## 5. Business case

This section provides the business case for care data. It begins by explaining why NHS England believes that these changes to the use of patients' data are so important and the value that the linked pseudonymised data and published aggregate data can bring to a wide range of people including patients, the public, health and social care providers, commissioners and researchers.

Health and care providers collect large quantities of data every day through their interactions with patients; however most providers and commissioners of currently care lack comprehensive information about the impact of their services on patient outcomes. Currently, there are no nationwide mechanisms to link health and social care data across all of the different settings where a patient may receive care (e.g., primary care, hospitals, community health services, and social care). As a result, the information available to patients, clinicians and planners is incomplete.

Care data will bring together patient-level information from all healthcare settings to generate a joined-up view of the care being provided to patients. Commissioners need this type of joined-up data to ensure that their patients are receiving seamless, integrated care and to

prevent unnecessary duplication and gaps in care provision. It is vital that commissioners and other stakeholders see a complete view of the care being provided to their population or provider setting, including care that spans across different care settings. Historically, patients who required care from multiple providers often experienced undue fragmentation and duplication in their care. Only by analysing linked information can commissioners ensure that their patients are receiving properly integrated care and clinicians ensure their care is of high quality.

The six purposes of care.data are:

- vii. Greater accountability
- viii. Informed choice
- ix. Greater efficiency
- x. Better outcomes
- xi. Customer services
- xii. Economic growth.

### **1. Greater Accountability**

Through the care.data programme, NHS England will help citizens to hold the NHS to account by making more information available about the quality, safety, and efficiency of the care provided. For example, we will make more information available about prescribing patterns so that citizens can see how equitable is the provision of drugs across England. We will do the same for waiting times, disease outcomes, and other metrics.

### **2. Informed Choices**

Better access to higher quality and more complete information will give patients the opportunity to exercise greater control over their care and wellbeing. For example, the document *'Liberating the NHS: An information strategy'*<sup>14</sup> lists the kinds of information that people will use, including information about:

- suitable medicines and treatments, together with their risks, benefits and side effects;
- clinical outcomes and success rates, such as readmission or mortality rates;
- other indicators of quality and performance, such as infection rates.

An important role of the care.data programme is to provide such information to patients and clinicians, and enable patients to make more informed choices. By doing so, patients and clinicians will be able to play a more effective part in improving the quality and efficiency of the health service.

NHS England is committed to making more information available to patients and citizens through the care.data programme, and we will encourage people to make greater use of this information. We will also be responsive by providing information that people say they want in the formats they want it in.

### **3. Better Outcomes**

Other than some local examples, there is little linkage of detailed level across primary and secondary care settings, so there is little opportunity to monitor patient outcomes. Linking data provides a more complete picture of the care so that analysts can look at the effect of

<sup>14</sup> <http://consultations.dh.gov.uk/information-revolution/informationrevolution>

an intervention or a particular route a patient took from diagnosis, through to treatment and discharge and see what worked best so that all patients can benefit.

To give an example: 20 patients have the same surgical procedure and are discharged by a hospital. The hospital has no further contact with the patients and therefore hospital analysts consider that the procedure was successful. However, the hospital was unaware that 10 of those patients visited their GP with complications, which were managed by the GP practice. By looking at the linked data, the hospital analysts would have had a more complete picture of patient outcomes.

#### **4. Customer Services**

We need to ensure patients are at the heart of the health and social care service and services are tailored to each individual's needs so they receive a first class customer service. Patients can use information about services to make informed choices about their healthcare. Eventually it is intended that patients can have access to their data including the data collected for care.data so they can share this for example, with healthcare providers, charities or their family and play an active role in shaping their own healthcare.

#### **5. Greater efficiency**

Detailed analysis of data can help improve efficiency through a variety of mechanisms, including:

- Ready access to high quality information can lead to improvements by allowing professionals to identify variances and inconsistencies in their practice compared to how other health care providers practice. For example, GPs may identify more efficient prescribing practices amongst their peers, and pathologists may identify practices in other laboratories that will help increase their productivity.
- As part of the care.data programme, NHS England will make more information available about the efficiency and performance of all parts of the NHS. Having ready access to this information will support NHS organisations to become more efficient and will help reduce the cost to individual organisations of obtaining and processing information about performance.
- Using risk models and decision aids can help ensure that care is provided to those who most need it or prevent unscheduled hospital admission eliminating waste and thereby improve efficiency.

#### **6. Economic Growth**

In order to safeguard the fundamental philosophy of providing high quality care to all, free at the point of delivery, the NHS requires a strong economy. The care.data will support economic growth in a variety of ways. For example:

- Greater access to high quality health and care data will help reinforce the UK as a global centre for life sciences and health services research. Making de-identified data available at scale will help researchers discover and refine new treatments. It will also help epidemiologists and public health researchers to shed more light on the role of social conditions and lifestyle choices on health outcomes.
- Making comparative data available to app developers and website designers will support the development of a vibrant market place.
- Offering a range of data services at regional and local levels will support economic growth by encouraging small and medium-sized enterprises (SMEs) to provide of innovative, locally-tailored analytical tools and services.



- Better information will support the modernisation of services, which in turn will support economic growth

## 6 Alternatives to identifiable data

The fundamental purpose and benefit of care.data is to collate and link health and social care data from a wide range of care settings in order to provide a more complete picture of the care received by patients. Put simply, in order to ensure that it is providing joined-up care, the NHS needs joined-up data. For example, in order to gauge the quality of services for patients who have had a hip fracture, clinicians, commissioners, and researchers need information about:

- what happened to patients while they being cared for
  - by the ambulance trust,
  - by the A&E department,
  - in the operating theatre and
  - on the hospital ward
- how well their care was coordinated after leaving hospital, and
- whether they maintained their independence.

In order to make a complete assessment of the outcomes for patients, we therefore need to link data from all of the settings at which they may receive care, including primary care, secondary care, tertiary care, community health services, and social care.

Clearly, it is essential that a patient's data from one care setting are correctly linked up with their data from another care setting. For the care.data programme, we use four separate identifiers to ensure that records are linked accurately. The identifiers are the patient's NHS number, date of birth, gender and postcode.

We have rejected alternative data linkage techniques using fewer identifiers because the scale of the linkage required (i.e. patient records for the whole population from a wide range of health and care settings) means that there are more individuals who share similar identifiers. Using fewer identifiers would lead to more incorrect linkages, which would compromise data accuracy and bring into question the validity of care.data. Moreover, using fewer identifiers would lead to a lower proportion of linked records, which would diminish the usefulness of care.data especially because of a bias in the characteristics of patients whose records that could not be linked.

Another option would be to de-identify the data at source in a consistent way that allowed individuals' data to be linked without revealing their "real world" identities. Known as *pseudonymisation-at-source*, this technique relies on the use of a common key across all care settings, which generates a unique pseudonym for each individual that allows their data to be linked. At the moment, the HSCIC considers pseudonymisation-at-source to be impractical because there is such a diverse range of care settings providing data to the programme (primary, secondary, tertiary, community, and social care) and such a diverse range of information systems used in each setting.

For all of these reasons, the HSCIC requires four identifiers in order to link the data accurately.



## 7 What will we do to protect privacy?

The care data programme is being delivered by the HSCIC, whose core purpose within legislation is to process patient records safely and securely. As stated in the HSCIC PIA "The HSCIC has been processing patient records safely and securely since its inception. It has introduced strong security controls, published and implemented security policies and published information about its processing as required for compliance with the Department of Health's Information Governance Framework.

The HSCIC takes its responsibilities as a custodian of patient information extremely seriously and is also committing to a number of pledges to protect privacy as set out below. In Appendix A, we describe how the privacy risks identified in section 4 are addressed by these controls and pledges.

### 7.1 Information Governance Controls

---

The HSCIC will collect, process, disseminate and publish data on behalf of NHS England for and care data programme. The HSCIC provides assurances regarding Information Governance through:

- An Information Assurance Steering Group, with reporting lines to the Executive Board
- satisfactory completion of the NHS Information Governance Toolkit<sup>13</sup>, and compliance with ISO27001/2 Information Security Standards, which include:
  - Staff training and contracts<sup>14</sup>
  - Information technology system security and audit trails
  - Robust management arrangements<sup>15</sup>
  - Full compliance with legislative requirements
  - Provision of the "safe haven" for sensitive information

Specifically the HSCIC will:

- 1) Obtain and process the minimum necessary patient identifiable data from other organisations;
- 2) Store and process identifiable data securely, meeting or exceeding the standards required of NHS organisations, including technology to:
  - i. De-identify data received as early as possible, and where records have to be linked; it will separate patient identifying data from clinical data, and assign a meaningless identifier (pseudonymisation)
  - ii. Store data in its capacity as the "safe haven" under the Health and Social Care Act 2012.
  - iii. protect against attacks from unauthorised individuals (e.g. hackers)
  - iv. protect against inappropriate behaviour by staff;
  - v. provide only legitimate personnel with access to HSCIC systems, and to no more access than they legitimately require;

3. Keep to the absolute minimum the number of staff able to access and view patient identifiable data, and wherever practicable assign staff rights of access to either patient identifiers or clinical data but not both;
4. Destroy data held in identifiable form as soon as they are no longer required, or in accordance with the retention policy;
5. Disclose only anonymised data, other than:
  - i. with explicit patient consent;
  - ii. where required by law, or
  - iii. where allowed by law, with necessary support and approvals, and either:
    - the support of the Independent Advisory Group; or
    - where urgent, with the agreement of both the Senior Information Risk Officer and Caldicott Guardian for HSCIC;
6. When disclosing anonymised data, restrict the data disclosed according to the context in which the data will be used:
  - i. When publishing statistics and other aggregated information, apply disclosure control standards<sup>25</sup> to ensure data are anonymised;
  - ii. When disclosing patient-level data to a trusted organisation:
    - confirm the data are anonymised by carrying out a risk assessment
    - maintain a written agreement with the recipient organisation that stipulates the permitted access to, and uses of, the data;
7. Monitor who accesses patient identifiable data.

## **7.2 Additional care.data pledges to protect information**

---

In addition to the information governance controls outlined above, further safeguards will be put in place to protect information collected, processed and disseminated as part of care.data. The two organisations will be held to account against these pledges by the Department of Health.

- A. The HSCIC will publish a Code of Practice to govern the use of confidential data supplied to the Health and Social Care Information Centre that encompasses care.data;
- B. The HSCIC and NHS England will respect the wishes of patients who request that their data are not used by care.data, unless there is a statutory duty or an overriding public interest (e.g. public health emergency) to do otherwise;

<sup>25</sup> The Health and Social Care Information Centre's current policy is available at: [http://www.hscic.gov.uk/media/1350/Publications-Calendar-Statistical-Governance-Policy/pdf/The\\_HSCIC\\_Statistical\\_Governance\\_Policy\\_v3.1.pdf](http://www.hscic.gov.uk/media/1350/Publications-Calendar-Statistical-Governance-Policy/pdf/The_HSCIC_Statistical_Governance_Policy_v3.1.pdf)

- C. The HSCIC will commission, at least annually, external information governance audit against information governance standards.
- D. NHS England and the HSCIC will be transparent about their activities and communicate openly, fairly and lawfully through the NHS England and HSCIC public websites and other channels where appropriate;
- E. The HSCIC will publish procedures for dealing with requests for information and operate effective policies and procedures to encourage good information governance by staff, with proportionate sanctions (e.g. dismissal) for inappropriate or negligent behaviour.

## 8 Public Acceptability

The HSCIC PIA describes how the government consulted stakeholders to inform the powers in the Health and Social Care Act<sup>16</sup>.

Personal confidential data have been used for purposes beyond direct care for many years such as for healthcare planning and for research. It is important that patients are clear about what information is being shared, how it is being shared and why so that they can understand the risks and benefits to them and to the wider population. Some patients may have particular concerns and therefore NHS England has made it simple for patients to object.

### 8.1 Independent scrutiny

The Independent Advisory Group (IAG) of the General Practice Extraction Service (GPES), considered the specification of the GP data. The group, which includes lay representatives, approved the extraction of GP data in order for it to be linked to hospital data and made available to commissioners.

NHS England and the HSCIC have worked closely with the British Medical Association and with the Royal College of General Practitioners during the process. We have listened to and incorporated views of these professional organisations, which culminated in publishing joint guidance and materials for GP practices.

### 8.2 Patient Information Materials

The BMA's Patient Liaison Group (PLG) was involved in commenting on the patient materials for informing patients about care.data. These materials, which included posters and leaflets, were then tested in a small number of practices over the summer of 2013. GP practice staff and patients were invited to provide feedback on the materials and NHS England communicated with these first practices in order to gauge public acceptability at this preliminary stage. Dialogue will continue with these practices as care.data is implemented on a national scale.

Information about the programme has been sent to over 350,000 patient groups, charities, and voluntary organisations. These organisations are being asked to cascade information

<sup>16</sup> HSCIC PIA section 2.3 ([http://www.hscic.gov.uk/media/12931/Privacy-Impact-Assessment/pdf/privacy\\_impact\\_assessment\\_2013.pdf](http://www.hscic.gov.uk/media/12931/Privacy-Impact-Assessment/pdf/privacy_impact_assessment_2013.pdf))

about care.data to their members through their usual channels, including social media. In addition, NHS England has been engaging with the *strategic partnership programme*<sup>17</sup>, which enables voluntary sector organisations to work in equal partnership with the Department of Health (DH), the NHS and social care to help shape and deliver policies and programmes.

A series of meetings are being held with patient groups to discuss care.data. Meetings have been held with stakeholders for example with the Association of Medical Research Charities, Cancer Research UK and the British Heart Foundation. This is an ongoing exercise and further meetings will be held over the coming weeks and months with patient groups and charities to discuss their views on the design and implementation of care.data.

NHS England and the HSCIC have listened to stakeholders and a leaflet about information sharing will be delivered to every household in England. We are also implementing a patient information line to support patients who have questions or concerns and we will monitor feedback.

## 9 Conclusions

Any processing or storage of identifiable patient data introduces potential risks of data misuse and breaches of privacy. Although they can never be eliminated, such potential risks are significantly mitigated by the robust information governance controls as set out in section 8 which are all designed to safeguard patients' privacy. The centrality of information governance to the care.data to meet or exceed all information governance standards provides greater assurance about privacy than most organisations are able to provide. Moreover, there is also a positive impact on privacy resulting from care.data de-identifying data. Making aggregated, anonymous and pseudonymous data available to commissioners, researchers and other approved bodies minimises their need to use identifiable data.

However, the processing of a person's information without their permission can be considered a loss of autonomy for that individual. For this reason, in addition to the extensive safeguards for the data, NHS England is supporting data controllers to raise awareness among patients and making it simple for patients to object to the disclosure of personal confidential data.

In summary, people who conclude that the net impact of care.data on privacy will be positive are very likely to be supportive of the programme. Even people who feel the impact will be detrimental to privacy may recognise that the potential benefits of care.data using data from patient records are great, and may therefore feel they are justified ethically on that basis. However, some people may believe that any use of patient identifiable data without explicit patient consent is unacceptable. These people are unlikely to be supportive of care.data whatever its potential benefits and may object to the use of personal confidential data for wider healthcare purposes.

The HSCIC will be processing data on behalf of NHS England and we have detailed the information governance and pledges in relation to care.data. The HSCIC PIA concludes 'While the HSCIC is new, its functions, including the safe and secure processing of data are well founded, tried and tested in previous constituent organisations. The patient, and

<sup>17</sup> <https://www.gov.uk/government/publications/the-department-of-health-voluntary-sector-strategic-partner-programme>

therefore protecting patient confidentiality, is at the heart of everything we do'. NHS England is committed to working in partnership with the HSCIC and shares this view.

## Appendix A - Managing Privacy Risk

### (i) - Types of privacy risk

The Information Commissioner's Office Privacy Impact Assessment Handbook<sup>18</sup> explains why privacy matters and identifies and describes four classes of privacy risk:

- privacy of personal information;
- privacy of the person;
- privacy of personal behaviour; and
- privacy of personal communications.

The care.data programme could potentially pose risks to the privacy of personal information (i.e. the first of these classes of privacy risk). The two sub-categories of risk to privacy of personal information are relevant:

- A. Risks to individuals as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information;
- B. Risks to organisations providing and/or using data within care.data as a result of:
  - I. perceived harm to privacy;
  - II. failure to meet public expectations on the protection of personal information (causing damage to the organisation's reputation);
  - III. failure to comply with the law, leading to enforcement action from the Information Commissioner; or compensation claims from individuals.

---

<sup>18</sup> [http://www.ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/privacy\\_impact\\_assessment](http://www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment)



## Risk Mitigation Matrix

Section 4 identifies a list of potential privacy risks and their potential impacts, and section 8 identifies information governance controls and pledges to reduce the risks to privacy. The table below indicates which risks each of the pledges is intended to address.

Control/Pledge to reduce risk/impact	Loss of autonomy	Confidential information viewed without consent	Misuse following illegal access	Misuse following lawful access
1) Obtain only the minimum necessary identifiable data	√	√		
2) Store and process identifiable data securely		√	√	√
3) Minimise which staff are able to view identifiable data	√	√		√
4) Destroy identifiable data when no longer necessary	√	√	√	
5) Disclose only anonymised data (other than where there are lawful exceptions)	√	√		√
6) Restrict what data are disclosed according to the context e.g. whether or not published	√	√		
7) Monitor who accesses patient identifiable data		√		
A. Publish a code of practice to govern the use of data			√	√
B. Respect patient objection	√	√		
C. Commission information governance audits		√	√	√
D. Be transparent and communicate fairly and lawfully	√	√		
E. Operate good information governance amongst staff with sanctions for misconduct		√	√	√

## Appendix B – Examples of use

The following are examples of how care data could be used:

### Example 1 - Colorectal cancer

Colorectal cancer is the third most common cancer after breast cancer and lung cancer, and is a major cause of mortality. Patients' chances of survival at five years are far higher when colorectal cancers are detected at an early stage (93%) versus those diagnosed late (6%); however, one quarter of colorectal cancer cases are diagnosed during emergency presentations to hospital.

The North East London Cancer Network identified a marked variability in the timeliness and accessibility of diagnostic services for patients with colorectal symptoms. The colorectal pathway is highly complex, with patients being referred to diagnostic services from both the community and by many different secondary care services.

High quality data are required to guide the development and implementation of care pathways, and to support patients and clinicians in making shared, informed decisions about treatment options. At a local level, GP data linked to hospital data are being used in a study that is examining variations in routes to diagnosis among patients with colorectal cancer in outer North East London. The project is exploring existing diagnostic pathways and aims to identify those pathways that result in the best outcomes for patients including the fewest avoidable healthcare episodes.

*What does this mean for patients?*

Every patient wants to be confident that they are receiving the best possible care. However, poorly designed pathways of care tend to result in more fragmented, inefficient care, and poor patient experience. By linking GP and hospital data, analysts can help to define what constitutes optimal care along coordinated care pathways. This information can then be used by NHS commissioners to reduce the variability in current pathways of care, thereby helping to ensure equal access to the best treatment options across the country.

The North East London Cancer Network is an example of how the care data dataset could be used to expand a local example of good practice into a service that could improve the quality, efficiency, and equity of care across the whole of England. By providing access to an individual-level, pseudonymised national dataset of linked GP and hospital data, researchers will be able to spend less time collecting and collating data and more time investigating patterns and trends, such as the time lags between diagnosis and treatment for a whole range of cancers and other diseases, together with any unwarranted variation in these lags across the country and between different patient groups.

Put simply, this means that the HSCIC would:

- link GP data to hospital data,
- then remove all identifiers and then provide these linked data to researchers in a way that does not identify individuals. □

The researchers could then use the data to calculate the time a patient presented with symptoms to the time they were treated, and the subsequent outcome of the treatment. □ An example: if patients in Bristol experience a 12 week delay from presentation to treatment compared with a 3 week delay for patients in Bath, then further research can take place to understand why there is a difference. What is the NHS in Bath doing differently from Bristol? Where are the delays occurring on the patient's journey? Are patients in Bristol having more

appointments? What can be learnt from Bath and applied to other areas? It is not necessary to know the identities of patients receiving care in Bristol or Bath to conduct this type of research, but it is necessary to combine the information from the GP practice and the hospital to look at these types of scenarios in detail. The lessons learnt could then be used to improve the delivery of services and care across the country.

### **Example 2 - using data to identify patients most at risk**

There is a clear benefit to patients and the public in ensuring that expert analysts can use data to develop models, which can identify patients that are most at risk, for example of unplanned hospital admissions, or patients who would most benefit from a particular treatment. Having more linked data available means that the accuracy of the models are improved.

*What does this mean for patients?*

Where predictive modelling is accurate it prioritises care for those who most need it. This results in better care for patients and a more efficient health and social care service.

### **Example 3 - Public Health England**

Public Health England (PHE) recently launched the world's largest single database of cancer patients. Containing clinical information on all 350,000 cancers diagnosed each year, this database will deliver near real-time cancer data to PHE analysts and epidemiologists. The dataset also offers exciting research opportunities (e.g. by allowing genome sequencing data to be linked to clinical data).

The registry currently receives data from all NHS Trusts. However, it is currently very difficult for PHE analysts to access national linked GP and HES data. They believe allowing them ready access to such linked data would be extremely beneficial, not least in understanding how best to improve cancer services across primary and secondary care.

The more information available to analysts and researchers about individual, pseudonymous, cancer patients, the greater their understanding of the disease epidemiology, treatment pathways, and outcomes. Therefore, nationwide linked GP- HES data is an extremely valuable addition to the PHE dataset.

*What does this mean for patients?*

Using the linked cancer dataset, researchers will be able to examine in detail the experiences of different sub-groups of cancer patients, for example to determine what treatments worked best. This information will then be used to inform the care of similar patients in future. The ultimate aim is to develop so-called stratified medicine (i.e., personalised treatment pathways for cancer patients based on their particular type of genetic mutation and other characteristics and preferences). In simple terms, this research could allow treatments to be more tailored to an individual (i.e. rather than medication for all patients with breast cancer, it would be medication for a subgroup of breast cancer patients, resulting in more effective treatment of the patient). In summary, this approach could deliver:

- increases in innovation and new treatment options,
- improved efficiency and better outcomes for patients
- increased patient understanding and choice of the different treatment options available to them.

## Appendix C – Definition of Terms

This document uses a variety of terms of particular relevance to privacy, and which could be open to more than one interpretation. To avoid the risk of misinterpretation, the table below contains a set of definitions. Wherever possible, it relies on existing published definitions, and in particular those in the Data Protection Act 1998, Section 251 of the NHS Act 2006<sup>15</sup> and in Confidentiality: NHS Code of Practice 2003<sup>16</sup> Where a definition is a partial extract from a lengthy published definition, the convention "... " is used below to denote this.

Term	Definition (or extract from full published definition)	Source
Aggregate data	Data derived from records about more than one person, and expressed in summary form, such as statistical tables.	Anonymisation Standard for Publishing Health and Social Care Data Specification.
Anonymisation	Any processing that minimises the likelihood that a data set will identify individuals. A wide variety of anonymisation techniques can be used; some examples of such processing are explained in this specification. Also commonly referred to as "de-identification".	Anonymisation Standard for Publishing Health and Social Care Data Specification
Clinical Audit	The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services.	Confidentiality: NHS Code of Practice <sup>19</sup>
Confidential patient information	"...patient information is "confidential patient information" where—  (a) the identity of the individual in question is ascertainable— (i) from that information, or (ii) from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information, and  (b) that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual."	Section 251 of the NHS Act 2006
De-identifying data	Any processing that minimises the likelihood that a data set will identify individuals. A wide variety of	Anonymisation Standard for Publishing Health and Social Care Data Specification

<sup>19</sup> <https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice>

	<p>anonymisation techniques can be used; some examples of such processing are explained in this specification.</p> <p>Also commonly referred to as "anonymisation".</p>	
Explicit consent	<p>"This means articulated patient agreement. A clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear."</p>	Confidentiality: NHS Code of Practice
Identifiable information	<p>A set of information from which a person (or persons) can be identified. Identifiable information is confidential, and so the definition for confidential patient information above also applies.</p> <p>Identifiable information can take a variety of forms, such as full patient records; extracts from records, and information not typically considered a record such as labelled laboratory samples.</p>	Confidentiality: NHS Code of Practice
Information governance	<p>Information Governance is to do with the way organisations 'process' or handle information. It covers personal information, i.e. that relating to patients/service users and employees, and corporate information, e.g. financial and accounting records.</p>	Information Governance Framework Standard <sup>20</sup>
Patient identifiable data	<p>Key identifiable information includes: □</p> <ul style="list-style-type: none"> <li>• patient's name, address, full post code, date of birth;</li> <li>• pictures, photographs, videos, audio-tapes or other images of patients; □</li> <li>• NHS number and local patient identifiable codes; □</li> <li>• anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.</li> </ul>	Confidentiality: NHS Code of Practice
Personal data	<p>*Data which relate to a living individual who can be identified:-</p>	Data Protection Act

<sup>20</sup> <http://www.isb.nhs.uk/library/standard/121>

	<ul style="list-style-type: none"> <li>- from those data; or</li> <li>- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller ☐</li> </ul> <p>and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".</p>	
Processing	<p>"Processing, in relation to information or data, means obtaining, recording or holding the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operations on the information or data, including—</p> <ul style="list-style-type: none"> <li>- organisation, adaptation or alteration of the information or data;</li> <li>- retrieval, consultation or use of the information or data (which, in relation to personal data, includes using the information contained in the data);</li> <li>- disclosure of the information or data (which, in relation to personal data, includes disclosing the information contained in the data) by transmission, dissemination or otherwise making available, or</li> <li>- alignment, combination, blocking, erasure or destruction of the information or data." ☐</li> </ul> <p>Note that a very similar definition for "processing" is used within the NHS Act 2006.</p>	Data Protection Act
Pseudonymisation	<p>A technique that replaces identifiers with a pseudonym that uniquely identifies a person. ☐ In practice, pseudonymisation is typically combined with other anonymisation techniques.</p>	Anonymisation Standard for Publishing Health and Social Care Data Specification
Public interest	<p>"Exceptional circumstances that justify overruling the right of an individual to</p>	Confidentiality: NHS Code of Practice



	<p>confidentiality in order to serve a broader societal interest.</p> <p>Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services."</p>	
Safe haven	A bounded secure environment suitable for the receipt, storage, transmission and other processing of any confidential information, including the most sensitive personal information. It may be a physical space (such as a secure room), a configuration of electronic devices or a combination of the two, where secure processes are enforced.	
Section 251 (or s251)	Refers to Section 251 of the National Health Service Act 2006. It provides the power to ensure that patient-identifiable information needed to support essential NHS activity can be used without the consent of patients. The power can only be used to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice.	NHS Information Governance – Guidance on Legal and Professional Obligations - DH/Digital Information Policy Sept. 2007
Sensitive personal data	The Act defines categories of sensitive personal data, namely, "personal data consisting of information as to:- (a) the racial or ethnic origin of the data subject; (b) his political opinions; (c) his religious beliefs or other beliefs of a similar nature; (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992); (e) his physical or mental health or condition; (f) his sexual life; (g) the commission or alleged commission by him of any offence; or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."	Data Protection Act