



**MEMORANDUM OF UNDERSTANDING**

**BETWEEN**

**HEALTH AND SOCIAL CARE INFORMATION CENTRE**

**AND**

**THE HOME OFFICE**

**AND**

**THE DEPARTMENT OF HEALTH**

## Contents

Paragraph Number	Title of Paragraph	Page Number
1	Participants to the Memorandum of Understanding	3
2	Introduction	3
3	Legal bases to disclose data	3
4	Role of Immigration Enforcement	4
5	Role of NHS Digital	5
6	Role of Department of Health	5
7	Justification of data disclosure	5
8	Freedom of Information and Subject Access Requests	8
9	Information handling	9
10	Process and method of exchange	10
11	Roles and Responsibilities of each Participant to the MoU	10
12	Media and Parliamentary handling	12
13	Review and amendments of the MoU	12
14	Costs	13
15	Retention and destruction schedule	13
16	Suspension	13
17	Termination	13
18	Issues, disputes and resolution	14
19	Signatories	14

## **1. Participants to the Memorandum of Understanding**

The Participants to this Memorandum of Understanding (MoU) are:

**THE SECRETARY OF STATE FOR THE HOME DEPARTMENT** (“Home Office”) of 2 Marsham Street, London SW1P 4DF

AND

**HEALTH AND SOCIAL CARE INFORMATION CENTRE (known as NHS DIGITAL)** (“NHS Digital”), a **NON-DEPARTMENTAL PUBLIC BODY (NDPB)** of the **DEPARTMENT OF HEALTH** of 1 Trevelyan Square, Boar Lane, Leeds, LS1 6AE

AND

**THE SECRETARY OF STATE FOR THE DEPARTMENT OF HEALTH** (“Department of Health”) of **Richmond House, 79 Whitehall, London, SW1A 2NS**

Collectively the Home Office, NHS Digital and the Department of Health will be referred to as “the Participants”.

## **2. Introduction**

2.1 The purpose of this MoU is to describe the protocol under which information requests submitted by the Home Office, the requestor, will be made to and processed by NHS Digital, the data discloser, in accordance with the legal provisions detailed in section 3 below, and the respective roles and responsibilities of each of the Participants.

2.2 This MoU is not a contract nor is it legally binding. It does not in itself create lawful means for the exchange of information; it simply documents the processes and procedures agreed between the Participants.

### **Date MoU comes into effect**

2.3 This MoU will come into effect on 1 January 2017.

## **3. Legal bases to disclose data**

3.1 Data can only be disclosed under this MoU where there is a legal basis and for the purposes described in this MoU. No data should be disclosed without a legal basis and all disclosures must comply with the Participants’ legal obligations under the Data Protection Act 1998 (DPA), the Human Rights Act 1998 (HRA) and the Health and Social Care Act 2012 (and any updates to these acts).

---

OFFICIAL

### Home Office to NHS Digital

3.2 As a Crown Government Department, the Home Office has common law powers which provide a legal basis for its disclosure of information, except in cases where there is a legal barrier to that disclosure.

### NHS Digital to Home Office

3.3 NHS Digital may disclose information under s.261(5) of the Health and Social Care Act 2012. Section 261(5)(e) provides a basis for disclosure where the disclosure is made in connection with the investigation of a criminal offence (whether or not in the United Kingdom); section 261(5)(d) provides a basis for disclosure where the disclosure is made in circumstances where it is necessary or expedient to have the information for the purpose of exercising its functions under or by virtue of any provision of any Act, and s.261(5)(c) provides a basis for disclosure where the disclosure is necessary or expedient for the purposes of protecting the welfare of the individual. These parts of s.261(5) are subject to the common law duty of confidentiality which is not absolute (see s.261(6)): the common law duty may be overridden in certain circumstances including where the public interest justifies disclosure.

## **4. Role of Immigration Enforcement**

4.1 Immigration Enforcement forms part of the Border, Immigration and Citizenship system. Its mission is to reduce the size of the illegal population and prevent harm caused by illegal migrants. Immigration Enforcement deploys a wide range of interventions to maximise the return of those here illegally, increase compliance and deterrence, and penalise those who facilitate and benefit from immigration abuse. These interventions include encouraging voluntary return by denying access to benefits and services to which they are not entitled; tackling those who work illegally, and those who employ them; applying hard edged enforcement capabilities – arrest, detention and deportation – to the most non-compliant and those presenting the most harm to the UK; prosecuting and disrupting organised immigration crime.

4.2 Immigration Enforcement's performance framework is based on five strategic objectives:

- Reduce the size of the illegal migrant population;
- Reduce the harm to the UK from illegal migration;
- Increase the number of foreign national offenders removed;
- Tackle the criminality behind immigration abuse; and
- Increase the number of illegal migrants leaving the UK.

4.3 The above is achieved through the implementation of a range of strategies, including clear messaging to migrants around the terms of their leave and contact with the Home Office and partnership working with a number of key stakeholders including other Home Office commands (e.g. Border Force, UKVI), the private sector, other Government departments and Local Authorities.

## **5. Role of NHS Digital**

5.1 NHS Digital is the national information, data and IT system provider to the health and care system.

5.2 NHS Digital's role is to improve health and social care in England by putting technology and information to work in the interests of citizens. NHS Digital builds and manages the technology infrastructure, digital systems, services and standards that health and care professionals depend on to deliver good care. NHS Digital gathers and disseminates data that is used by researchers to discover new treatments and generates information that helps providers and commissioners improve care quality.

5.3 NHS Digital has a statutory duty to ensure that the information it holds in trust for the public is always kept safe, secure and private.

## **6. Role of Department of Health (DH)**

6.1 DH is a ministerial department supported by 14 arm's length bodies including NHS Digital and a number of other agencies and public bodies. DH leads, shapes and funds health and care in England, making sure people have the support, care and treatment they need, with the compassion, respect and dignity they deserve.

6.2 DH's responsibilities include:

- Leading across health and care by creating national policies and legislation, providing the long-term vision and ambition to meet current and future challenges, putting health and care at the heart of government and being a global leader in health and care policy;
- Supporting the integrity of the system by providing funding, assuring the delivery and continuity of services and accounting to Parliament in a way that represents the best interests of the patient, public and taxpayer; and
- Championing innovation and improvement by supporting research and technology, promoting honesty, openness and transparency, and instilling a culture that values compassion, dignity and the highest quality of care above everything.

## **7. Justification of data disclosure**

7.1 This MoU sets out the circumstances in which the Home Office (in accordance with relevant legal basis) may make requests of NHS Digital for information which may then be used for the purposes set out below, how such requests are to be made, and what information may be provided in return (in accordance with the relevant legal bases).

7.2 Home Office staff may make requests to NHS Digital to establish if they hold certain non-clinical information (defined at Annex A) in relation to immigration offenders, and if so for that information to be provided to the Home Office for the express purpose of supporting its strategic priorities and solely where in accordance with one or more of the purposes set out within section 261(5) (c), (d) and (e).

7.3 In particular, the Home Office seeks information from NHS Digital pertaining to immigration offenders who are:

- Not in contact with the Home Office and the Home Office has no knowledge of any reasonable excuse for this; **and:**
- Are sought in regard to an immigration offence under Section 24 or 24A of the Immigration Act 1971, including where they have:
  - I. Failed to comply with reporting restrictions (including any grant of bail, temporary admission or temporary release); or
  - II. Absconded from port immigration control; or
  - III. Escaped from detention; or
  - IV. Exceeded their time limit to stay in the UK; or
  - V. Sought to obtain leave by deception.
- Or would have been sought for such an offence save for this not being possible by virtue of the individual's age, and the Home Office believes the individual is at risk, and section 7.5 shall apply.

7.4 Subject to section 7.5, the Home Office only agrees to request information from NHS Digital in cases where the Home Office:

- Confirms the requested information is necessary for the purposes of the prevention or detection of crime or the detection, apprehension or prosecution of offenders and failure to supply that information would prejudice the investigation and those purposes, in accordance with Section 29(3) of the Data Protection Act 1998 (save where the individual concerned is below the age of criminal responsibility);
- Confirms that the disclosure of the requested information by NHS Digital is for a purpose permitted by Section 261(5) of the Health and Social Care Act 2012;
- Confirms the s.24/s.24A offence(s) that the immigration offender has committed or is suspected of committing (save where the individual concerned is below the age of criminal responsibility);
- Confirms that disclosure of the information by NHS Digital is a matter of public interest;
- Confirms that the Home Office has utilised all usual sources of internal information as a means of re-establishing contact with the person and has taken all reasonable steps in accordance with normal Home Office

procedures, to locate and re-establish contact with the person via other appropriate, centrally held, Government sources of information;

- Provides information about (including the statutory reference) any other offence that the person is sought in regard to (where relevant);
- Includes any last known address for the immigration offender (so as to confirm existing UK residency status); and
- Confirms that the Home Office will not make a request to NHS Digital immediately on a person becoming an immigration offender (unless exceptional circumstances apply, such as safeguarding or public safety concerns), but rather will make a request where the person concerned is not in contact with the Home Office and other reasonable and appropriate efforts to locate them have failed.

7.5 Notwithstanding the preceding provisions, the Participants agree that the Home Office may submit a request for information that falls outside the parameters in section 7.4 where:

- The Home Office has evidence to suggest NHS Digital may be the sole source of the information requested; or
- In the interests of public safety, or the welfare of an individual.

And the public interest in disclosure outweighs the public interest in maintaining any confidentiality.

7.6 The Home Office will provide additional information to justify a request where it is appropriate and relevant to do so.

7.7 The Home Office will use the agreed request template at Annex B and requests will only be made where the Home Office has examined the case and determined that the disclosure is in the public interest. Any information received as a result of the data disclosure will be used in conjunction with other information already held by the Home Office or obtained by the Home Office.

### Public Interest

7.8 There is public interest in disclosing data on all offenders under s.24/s.24A of the Immigration Act 1971. The commission of a criminal offence of this type is a matter of high public interest.

7.9 Additionally, the importance of maintaining effective immigration controls and the work of immigration enforcement has been recognised in Parliament, by the courts and internationally. It enables the government to remove/prevent the entry of those who might pose a danger to the public. Furthermore, and given immigration offenders also harm the economic wellbeing of the country, it is in the public interest that limited UK resources and public services (including the NHS, jobs, schools, housing) are protected from unnecessary financial and

resource pressures. Parliament has clearly stated the importance of maintaining effective immigration control and that this is in the public interest. In many cases, immigration offenders are either removed or deported from the United Kingdom and/or have restrictions placed on their return.

7.10 The nature of the offences are such that there is a low probability of mistaken identity.

7.11 The information to be disclosed under this MoU is administrative in nature, and consequently falls at the less intrusive end of the privacy spectrum, making disclosure easier to justify as the public interest threshold is lower<sup>1</sup>.

7.12 There is also public interest in disclosing data, which as noted above is at the lower end of the privacy spectrum, in the interests of public safety or where there are concerns regarding the safety or welfare of an individual, such as a vulnerable child or adult.

## **8. Freedom of Information and Subject Access Requests**

### Freedom of Information (Fol) Requests

8.1 Home Office, DH, and NHS Digital are subject to the requirements of the Freedom of Information Act 2000 (FoIA) and shall assist and co-operate with each other to enable each Participant to comply with their information disclosure obligations.

### Fol requests for information held by receiving Participant

8.2 In the event that an Fol request is received and only relates to information held by the receiving Participant, it will issue a formal response following their internal process and procedures for responding to Fol requests within the statutory timescales.

### Fol requests for information held by another Participant

8.3 Where it is identified that the Fol request (in its entirety) relates to information held by another Participant to this MoU; the receiving Participant will issue a formal response informing the requestor that the information requested is held by the other Participant(s) and provide the relevant contact details for the other Participant(s). (See Annex E)

### Cross Government Fol Requests

8.4 Where it is identified that a Fol request relates to information held partly by two or more Participants to the MoU, the receiving Participant will issue a formal

---

<sup>1</sup> Note: In W, X, Y & Z [2015], the court stated: "The fact that the disclosure may be 'less intrusive' than disclosure of detailed information about an individual's medical condition and treatment does not mean that it is not intrusive at all or that the information is not inherently private. Instead, it means that it is likely to be easier to justify disclosure".

response answering only the questions that are applicable to their own department and refer the requestor to the other Participant(s) that holds the information on the remaining questions; where available, contact details for the other relevant Participant(s) can be provided in their response. Where it is identified that a FoI request relates to information held by the receiving Participant but is owned by the other Participant, the receiving Participant will issue a formal response but shall first consult with the other Participant to ensure there are no objections to the disclosure.

#### Subject Access Requests (SAR) under the Data Protection Act 1998 for information held by receiving Participant

8.5 In the event that a SAR is received and only relates to personal information held by the receiving Participant; the receiving Participant will issue a formal response following their internal process and procedures for responding to the SAR within the statutory timescales.

#### SAR requests for information held partially by receiving Participant

8.6 Where it is identified that the receiving Participant does not hold all the information requested, they are only expected to disclose the information they have available, in accordance with their obligations under the DPA. There is no statutory requirement to re-direct SARs or provide details of other Government departments or Participants in the response.

### **9. Information handling**

9.1 Home Office and NHS Digital are data controllers, and as such are subject to the Data Protection Principles set out in the DPA. Additionally as part of Her Majesty's Government, the Home Office must process personal data in compliance with both the mandatory requirements set out in the Communications Electronic Security Group (CESG) Handling Personal Data Guidance May 2013 (Annex C) and the Security Policy Framework (SPF) issued by HM Cabinet Office April 2014 when handling, transferring, storing, accessing or destroying information assets. The SPF can be accessed via the following link to the Gov.UK website: <https://www.gov.uk/Government/publications/security-policy-framework> – NHS Digital must process personal data in compliance with the Health and Social Care Act 2012 and the NHS Information Governance Tool Kit: <https://www.igt.hscic.gov.uk/>

9.2 The Home Office and NHS Digital will expect the other to have taken every reasonable measure to comply with the appropriate data security and information governance standards, and may conduct a risk assessment of the exchange against these requirements.

9.3 The disclosing Participant will ensure that data integrity meets their department's standards.

9.4 The Home Office and NHS Digital must report any information losses, wrongful disclosures or breaches of security relating to information disclosed under the terms of this MoU, to the designated contacts provided at Annex E immediately (within 24 hours of becoming aware). This includes advising, and consulting with, the other Participant on the appropriate steps to take; e.g. notification of the Information Commissioner's Office (ICO).

## **10. Process and method of exchange**

10.1 The process and method of exchange is set out in Annex A of this MoU.

## **11. Roles and Responsibilities of each Participant to the MoU**

### Home Office

11.1 To ensure all aspects of the MoU are adhered to, the Home Office shall:

- Identify the appropriate information required for the tracing request from Home Office records;
- Use the agreed tracing request proforma (provided at Annex B) when submitting a request to NHS Digital. This is necessary to enable NHS Digital to fulfil its Common Law obligation to assess public interest or any additional information as required under s.261(5) or other legal provision;
- Use the agreed contact points to send the tracing request to NHS Digital as stipulated in Annex A;
- Send the request via secure GSI email network with the subject line marked as "OFFICIAL" in accordance with the Government Security Classification Scheme (GSCS);
- Make any tracing requests in accordance with the provisions of this MoU and for the purpose set out herein;
- Ensure all information requests are approved by an appropriate IE official of Higher Executive Officer (HEO) grade or above;
- Make a tracing request when the request has been assessed and the request is deemed to be in the public interest;
- Only retain the information that is identified and disclosed by NHS Digital for as long as there is a business need in accordance with s.261(5) of the Health and Social Care Act 2012; and
- Agrees that from time to time it will undertake analysis as to the value of tracing for immigration control purposes, and to share the results of this analysis with the Participants to this MoU.

---

OFFICIAL

## NHS Digital

11.2 In its provision of the information NHS Digital shall:

- Identify the appropriate information required by Home Office from its records;
- Only use the agreed tracing request proforma when returning the results of the tracing check to the Home Office;
- Send the results of the tracing check to the originator;
- Send the results of the tracing check via secure NHS mail with the subject line marked as “OFFICIAL” in accordance with the GSCS;
- Aim to respond to a tracing request within the agreed timeframe of 20 working days; and in exceptional circumstances (for example where there are concerns over the wellbeing of children) NHS Digital acknowledges the Home Office may request a response in a shorter time frame and the time frame will be agreed on a case-by-case basis with NHS digital and provided on the tracing request proforma at the time of the request;
- Retain the right to seek more information from Home Office should they need to; and
- Without limitation, NHS Digital may refuse a request for information from the Home Office if it is not satisfied that the request is in the public interest.

## Department of Health

11.3 To ensure all aspects of the MoU are adhered to, the Department of Health shall:

- Maintain oversight of the progress of data flows via accountability arrangements between DH and NHS Digital, including updating Ministers when required, and
- Broker solutions between NHS Digital and Home Office should any resultant issues arise. The responsibility resides with NHS Digital and Home Office to inform DH of any such issues.

## Legal Challenge

11.4 In the event of a legal challenge against any of the Participants, relating to the disclosure of information under the terms of the MoU, the Participants agree to cooperate in preparing and sharing information necessary to demonstrate the basis on which the challenged disclosure was made. For the avoidance of

---

OFFICIAL

doubt, no Participant shall be required to share information that is subject to legal privilege.

11.5 Any legal challenge is to be managed by the Participant that is the appropriate defendant in the proceedings in consultation with the other Participants, with costs and any damages to be shared on the basis of 50% the Home Office, and 50% the Health Participants, subject to the following conditions:

- The other Participants are only required to make a payment where costs and any damages reach or exceed £3,000 within any 12 month period, starting with the commencement date; and
- The costs of any legal challenge that is commenced before the termination or suspension will continue to be shared between the Participants until the conclusion of the legal challenge.

11.6 Subject to the provisions of section 11.5, the Participants shall share information on costs and any damages, on a monthly in arrears basis where costs and damages has exceeded £3,000 in relation to any legal challenge. Participants shall forecast expected costs, and shall update the forecast information on a monthly basis, and shall share such forecast information with the other Participants.

## **12. Media and Parliamentary handling**

12.1 The Department of Health, Home Office and NHS Digital will look to ensure, as far as possible, mutual agreement of media handling including lines to take as and when required for response to media requests.

12.2 The Department of Health, Home Office and NHS Digital agree to provide each Participant with the required information as and when needed to assist with timely response to Parliamentary Questions.

## **13. Review and amendments of the MoU**

13.1 This MoU will commence in accordance with section 2.3 above, and will be renewed by the written agreement of the Participants on an annual basis. Any changes deemed to be necessary in the interim may be agreed in writing by the Participants and appended to this MoU for inclusion at the following review.

13.2 Reviews outside of the schedule can be called by representatives of any of the Participants.

13.3 External changes affecting the operational delivery responsibilities of the Participants will also necessitate the review and potential amendment of this MoU.

13.4 Amendments to this MoU may only be made upon written agreement between the Participants.

#### **14. Costs**

14.1 No charges will be made by either participant in relation to this MoU, and the data disclosure arrangement described within it, subject to 11.5 above.

#### **15. Retention and destruction schedule**

15.1 Participants will ensure that the information exchanged as a result of this MoU will not be kept longer than is necessary for the purpose set out in this MoU. Once this information is no longer relevant for the purpose set out in this MoU it will be destroyed securely in accordance with the relevant Participant's own retention and destruction policies.

15.2 All information received by Home Office from NHS Digital will be processed in line with Home Office retention, destruction and storage policies.

15.3 All information received by NHS Digital from Home Office will be processed in line with NHS Digital retention, destruction and storage policies.

#### **16. Suspension**

16.1 Notwithstanding any other provision of this MoU, NHS Digital shall be entitled to temporarily suspend provision of all or part of the services under this MoU by providing written notice to the Home Office and DH.

16.2 Where reasonably practical, NHS Digital will provide the Home Office and DH with a notice period of at least 5 working days before the suspension of all or part of the services under this MoU commences.

16.3 The written notice to the Home Office of intention to suspend all or part of the services under this MoU must include the reasons for the suspension, the date the suspension is due to commence and information on the steps that may need to be taken to prevent the suspension from taking place.

#### **17. Termination**

17.1 Participants to this MoU reserve the right to terminate this MoU with reasonable notice in the following circumstances:

- For material breach by any Participant of any of the terms of the MoU;
- By reason of cost, resources or any other factors beyond the control of any of the Participants; and

- If any material change occurs which, in the opinion of the Home Office or NHS Digital, following negotiation, significantly impairs the value of the data disclosure in meeting their respective objectives.

## **18. Issues, disputes and resolution**

18.1 Where a problem arises it should be reported immediately, to the designated operational contacts (listed in Annex E). The contacts will endeavour to resolve the problem within 2 working days. Once any potential changes have been identified, a formal change notification should be sent to the 'Data Exchange Coordinator'.

18.2 Where it is not possible to resolve the issue within 2 working days or the issue is of such severity that individuals may be negatively affected, the issue will be escalated to a senior representative for the Participant. They will be notified with an explanation of why the dispute has not been resolved so that they can take appropriate action for resolution or plan contingency arrangements.

18.3 Any issues regarding ongoing delivery aspects of the information supply, such as data integrity or quality, should be addressed through 'business as usual' channels as detailed in Annex E.

18.4 Where the 'business as usual' channels fail to reach agreement, the Participants will attempt to negotiate a settlement in the spirit of joint resolution within 20 working days of a first notification being received as described in Section 18.1.

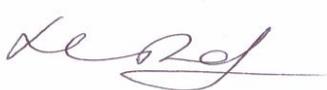
18.5 External changes affecting the operational delivery responsibilities of the departments will also necessitate the review and potential amendment of this MoU.

## **19. Signatories**

19.1 This MoU is confidential to the signatories.

### **19.2 Signed on behalf of the Home Office:**

I accept the terms of the MoU on behalf of the Home Office.

Signature:	
Name:	Hugh Ind
Date:	1 November 2016
Position:	Director General, Immigration Enforcement

---

OFFICIAL

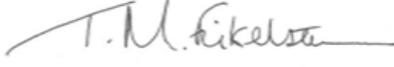
**19.3 Signed on behalf of NHS Digital:**

I accept the terms of the MoU on behalf of NHS Digital.

Signature:	
Name:	Andy Williams
Date:	1 November 2016
Position:	Chief Executive Officer

**19.4 Signed on behalf of the Department of Health:**

I accept the terms of the MoU on behalf of the Department of Health.

Signature:	
Name:	Tamara Finkelstein
Date:	2 November 2016
Position:	Director General, Community Care

## **Annex A – Process and method of exchange**

### Data to be disclosed

A1 On a case-by-case basis the Home Office will disclose the following data to NHS Digital on individuals where the Home Office suspects that an immigration offence has been committed under s.24 or s.24A of the Immigration Act 1971.

- NHS Number (if known)
- Surname
- Former/Maiden name (if known)
- Forename
- Middle name(s) (if known)
- Aliases (if known)
- Date of Birth
- Gender (if known)
- Last known address (including postcode)
- Previous 5 known addresses (including postcode) (if known)
- Nationality
- CID Person ID

A2 NHS Digital will match this data against NHS Digital records and then in response disclose to the Home Office the following data (where held) relating to those individuals that matched NHS Digital records:

- Surname
- Forename
- Middle names
- Date of Birth
- Gender
- Last known address (including postcode)
- CID Person ID
- Primary care service (PCS) area code and relevant contact details
- The date of their NHS registration
- Confirmation of death, registration district, year and quarter.

### Physical method of transfer

A3 The Home Office will provide NHS Digital with the information listed at A1 using the agreed tracing request proforma (see Annex B). The proforma will contain details of the individual the Home Office wishes to trace against NHS Digital records for the purposes set out in this MoU.

A4 All requests will be made in writing and sent by secure GSI email to NHS Digital designated inbox at [nbo-t4@nhs.net](mailto:nbo-t4@nhs.net) with the subject line marked as 'OFFICIAL' in accordance with the GSC marking scheme.

A5 All requests will be checked for appropriateness and signed off by a member of staff of at least Higher Executive Officer (HEO) grade.

---

OFFICIAL

A6 NHS Digital will aim to respond to each request within 20 working days of receipt and in exceptional circumstances as explained in Section 11.2 in a shorter time frame agreed with NHS Digital provided at the time of the request.

A7 NHS Digital will respond to the Home Office requestor via secure email using one of the Tracing Service's pre-prepared response proforma. If there is no positive trace, NHS Digital will confirm this in their response.

A8 NHS Digital will transfer the tracing proforma by secure email directly to the to the email address the request originated from.



Home Office

## Annex B: Home Office Request for the Disclosure of Personal Data

To	NHS Digital
Department	National Back Office
Address	Smedley Hydro, Southport, PR8 2HH
Email	<a href="mailto:NBO-T4@nhs.net">NBO-T4@nhs.net</a>
Telephone	0300 365 3664
Reference (CID ID of Subject)	

I, the undersigned, being an officer of the Home Office of Higher Executive Officer (**HEO**) grade or above, request the disclosure of Personal Data as set out in Part 5, Section B below (the **Requested Information**) on the individual identified in Part 5, Section A below (the **Subject**) for the purposes of exercising my functions under the Immigration Acts; under one of the categories below:

	Tick all appropriate
<b>Category 1 – Applications concerned with the investigation of a criminal offence;</b> <b>Now complete Sections 1, 4 (if appropriate), 5 &amp; 6 of this form.</b>	<input type="checkbox"/>
<b>Category 2 – Applications concerned with the welfare or protection of an individual;</b> <b>Now complete Sections 2, 4, 5 &amp; 6 of this form.</b>	<input type="checkbox"/>
<b>Category 3 – Applications where disclosure is otherwise necessary or expedient for the purpose of the exercise of functions by the Home Office under the Immigration Acts.</b> <b>Now complete Sections 3, 4, 5 &amp; 6 of this form.</b>	<input type="checkbox"/>



Home Office

**Section 1 – Section 29(3) Data Protection Act 1998 (Complete for all Category 1 cases)**

I confirm that the requested information is necessary for the prevention or detection of crime, and/or the apprehension or prosecution of offenders.

And that failure to disclose the Requested Information would in my opinion be likely to prejudice the investigation of those Purposes, in accordance with Section 29(3) of the Data Protection Act 1998.

I further confirm that I am making this request in the exercise of functions under the Immigration Acts. I further acknowledge that this request will be considered by NHS Digital in accordance with section 261(5)(e) of the Health and Social Care Act 2012.

The Subject is now sought by the Home Office in regard to the commission of the following criminal offence:

Insert Offence

If Other is selected, please provide full details of the offence:

which is an offence under Section 24 and / or 24A of the Immigration Act 1971 (the 1971 Act). And that the Subject, having either entered the UK illegally or only having limited leave to remain in the United Kingdom has, without reasonable excuse, failed to maintain contact with a designated officer<sup>1</sup>.

I confirm that I know of no reasonable excuse that would otherwise mitigate the Offence and that contact with the Subject has been broken as a consequence of the Subject's own action rather than that of the Home Office.

I further confirm that I have taken all reasonable steps in accordance with normal Home Office procedures, to locate and re-establish contact with the Subject via other appropriate, centrally held Government information; but not limited to: internal Home Office sources, DWP, HMRC, Police, their Employer, before making this disclosure request.

I confirm that the Subject has been under investigation by Immigration Enforcement since

**Additional Information**

- I confirm that the Subject is also sought in connection with other criminal offences as follows: (please detail the relevant legislation including the relevant section(s) and description of any other offence(s) committed below:

I confirm that it is my reasonable belief that disclosure of the Requested Information to the Home Office is in the public interest for the Purposes stated above.

<sup>1</sup> Defined in the Immigration Act 1971 as: medical officer of health; chief administrative medical officer of a Health Board; the chief administrative medical officer of a Health and Social Services Board; Police Officer; Immigration Officer; or the Secretary of State.



Home Office

**Section 2 – Welfare and or protection of an Individual (Complete for all Category 2 cases)**

I confirm that this requested information is necessary;

- due to the harm which could be caused to himself / herself if the Subject is not traced.
- due to the harm which could be caused to other individuals if the Subject is not traced.

I confirm the disclosure is necessary or expedient for the above purpose and failure to disclose the Requested Information would in my opinion be likely to prejudice an investigation currently being undertaken to locate the Subject.

I confirm that I am making this request in the exercise of functions under the Immigration Acts. I acknowledge that this request will be considered by NHS Digital in accordance with Section 261(5)(c) of the Health and Social Care Act 2012.

**Section 3 – Disclosure is necessary or expedient for the purpose of exercising functions under the Immigration Acts (Complete for all Category 3 cases).**

I confirm that it is necessary or expedient for me to have the Requested Information for the purpose of exercising my functions conferred by or under any provision of the Health and Social Care Act 2012 or the Immigration Acts, namely:

I confirm the disclosure is necessary or expedient for the above purpose and failure to disclose the Requested Information would in my opinion be likely to prejudice an investigation currently being undertaken. I acknowledge that this request will be considered by NHS Digital in accordance with section 261(5)(d) of the Health and Social Care Act 2012.

**Section 4 – Supporting information**

**This section MAY be completed for an application under Category 1 (investigation of an offence).**

**The section MUST be completed for every application under Category 2 (welfare) or Category 3 (statutory purpose). Without supporting information NHS Digital will have insufficient information on which to undertake the balancing exercise.**

To assist NHS Digital's consideration of this application, particularly those concerning welfare and or protection matters, the following supporting information is provided:



Home Office

<b>Section 5 (A) – Subject Details –</b> <i>Requestor to complete</i>	
<b>NHS Number (if known)</b>	
<b>Surname*</b>	
<b>Former/Maiden name (if known)</b>	
<b>Forename*</b>	
<b>Middle name(s) (if known)</b>	
<b>Aliases (if known)</b>	
<b>Date of Birth*</b>	
<b>Gender (if known)</b>	
<b>Last known address (including postcode)*</b>	
<b>Previous address 1 (including postcode)</b>	
<b>Previous address 2 (including postcode)</b>	
<b>Previous address 3 (including postcode)</b>	
<b>Previous address 4 (including postcode)</b>	
<b>Previous address 5 (including postcode)</b>	
<b>Nationality*</b>	
<b>CID Person ID*</b>	
Fields marked * are mandatory. If this information is not provided the request may be rejected.	

<b>Section 5 (B) – Requested information –</b>
<i>NHS Digital will provide the following information, where available, as agreed in the MoU.</i>
<b>Surname</b>
<b>Forename</b>



Home Office

<b>Middle name(s) (if known)</b>
<b>Date of Birth</b>
<b>Gender (if known)</b>
<b>Last known address (including postcode)</b>
<b>CID Person ID</b>
<b>Primary care service (PCS) area code and relevant contact details</b>
<b>The date of GP/Primary care registration</b>
<b>Confirmation of death, registration district, year and quarter</b>

### **Section 6 – Declarations and Signatures**

I confirm that the information I have provided above is to the best of my knowledge and belief true and I acknowledge and agree that in the event that the Requested Information is provided to me, it will be kept confidential and its use will be subject to the provisions of the Memorandum of Understanding agreed between the Minister of State; Home Office, NHS Digital and the Secretary of State for Health, dated 03/11/2016.

Name	_____
Grade (Minimum of HEO)	_____
Department	_____
Address	_____
Email address (Must match name and be used to submit request to NHS Digital)	_____
Telephone	_____

## Annex C: **CESG IA Top Tips 2013/02**

### **Handling Personal Data**

1. This guidance summarises requirements for the management of personal data following the withdrawal of HMG Information Assurance Standard 6.
2. It is important to note that personal data should be protected using a proportionate, risk managed approach, in the same manner used to protect all other types of information stored or processed by Departments, Agencies and their supply chain. The majority of the requirements contained in this document should therefore be familiar and applicable to protecting all types of information assets.
3. This document does not cover the legal requirements associated with protecting personal data. Departments and Agencies should consult the Information Commissioner's Office (ICO) website<sup>1</sup> to understand how to fulfil their legal obligations when processing personal data. Serious breaches of the Data Protection Act, which result in the loss, release or compromise of personal data, should be reported to the ICO.
4. The following are important considerations when handling personal data:

#### **Governance**

5. Departments and Agencies should appoint and train Information Asset Owners (IAOs) to understand and address the risks to their information assets, including personal data.

#### **Privacy Impact Assessments**

6. For all new policies or projects that include the use of personal information Departments and Agencies are required to assess the privacy risks to individuals in the collection, use and disclosure of information. This takes the form of a Privacy Impact Assessment (PIA), the nature and depth of which is determined by applying the screening process as detailed in ICO guidance, but should include a privacy law compliance check, which is available on their website. The PIA should form part of the risk assessment process as described in HMG Information Assurance Standard Nos. 1 & 2 (IS1 & 2), Information Risk Management.

#### **Information Charters**

7. Departments are required to publish an Information Charter setting out how they handle personal information and how members of the public can address any concerns that they have about how their information is handled. Guidance on the creation of an Information Charter is available from the Cabinet Office.

---

<sup>1</sup> [http://www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx)

## **Off-shoring of Personal Data**

8. In all cases, Departments and Agencies are required to seek approval from the Office for the Government Senior Information Risk Owner (OGSIRO) for any proposed off-shoring activity regardless of whether the data involved is personal in nature or not. Where approval for off-shoring personal data has been given, this must be within the European Economic Area (EEA) or a recognised equivalent (such as US-EU Safe Harbor).

## **Training**

9. Departments should ensure that all staff receive security training appropriate to their role. In particular, staff with access to personal data should successfully complete information risk awareness training on appointment to the post and as appropriate thereafter.

## **Access Control**

10. Staff who have a requirement to access, transfer or process information assets, including personal data, should only be granted the minimum access rights or functionality necessary to support business activities.

## **Protective Monitoring**

11. Departments and Agencies should ensure that appropriate arrangements are in place to log the activity of users processing sensitive information, including personal data, and that these logs are reviewed regularly. Particular attention should be paid to staff who are working remotely or who have access to higher levels of functionality / broader levels of access. Further guidance on the subject is available in CESG Good Practice Guide 13 (GPG 13), Protective Monitoring for HMG ICT Systems.

## **Transfer and Storage of Personal Data**

12. The transfer of sensitive information, such as personal data, over an untrusted network or via removable media should be protected proportionately using an appropriate grade of encryption. In situations where this is not possible a risk managed decision should be taken and the permission of the SIRO or IAO obtained.
13. Departments and Agencies should include guidance on when it is appropriate to use removable media to store or transfer information assets (e.g. personal data) as well as the minimum security controls required, in a removable media policy. The use of removable media to transfer or store personal data should be seen as a last resort. The amount of data transferred should therefore be limited to the minimum necessary to satisfy the business need.
14. The use of privately owned devices to store or access information assets presents a number of challenges, including how the device will be managed, whether the data held on the device can be adequately protected and if the data held on the personal device can be securely sanitised. There are also a number of legal issues surrounding the use of privately owned devices to store or process personal data for work purposes, which are discussed on the ICO website. The risks associated with privately owned devices are explained in greater detail in CESG Good Practice Guide 10 (GPG 10), Remote Working. CESG strongly recommends that users are not permitted to store or access personal data on such devices.

### **Incident Reporting**

15. Departments and Agencies must have an Incident Reporting policy and process in place and ensure that all staff are aware of that process.

### **Aggregation**

16. Departments and Agencies should note that aggregated information could attract Threat Sources/Actors with an increased motivation and/or capability as well as result in an increased impact should a compromise occur. The management of aggregated information assets should be determined by a risk assessment to ensure that appropriate controls are implemented.

### **Destruction**

17. All media used for storing or processing protectively marked information must be disposed of or sanitised in accordance with HMG Information Assurance Standard No. 5 (IS5), Secure Sanitisation, this includes personal data.

## Annex D – MoU document Control

### MoU Control Personnel

Key personnel	Name	Organisation (Team)
Author		Home Office
Approver	David Hughes	Home Office NHS Digital
Review Control		Home Office NHS Digital

### Version and review History

Version/review	Date	Summary of changes	Changes marked
Initial Draft V0.1	04/08/16	Initial draft	No
Second Draft V0.2	15/08/16	Incorporating IE changes and comments	No
Third Draft V0.3	19/08/16	Incorporating HOLA comments	No
Fourth Draft V0.4	30/08/16	Incorporating DH, IE and NHS comments	No
Fifth Draft V0.5	13/09/16	Incorporating DH, IE and NHS comments	No
Sixth Draft V0.6	16/09/16	Incorporating minor revisions	No
Seventh Draft V0.7	20/09/16	Incorporating DH, IE and NHS comments	No
Eighth Draft V0.8	21/09/16	Incorporating DH, IE and NHS comments	No
Final V1.0	27/09/16	Final Draft	No

## Annex E – Business Contacts

### Business as Usual Contacts – Home Office

Contact	Email	Responsibility
		Operational Queries
		Media/Press Enquiries
		Legal Issues
		Data Exchange Coordinator
		Security Incidents
		Parliamentary Questions
		Freedom of Information Requests

### Business as Usual Contacts – NHS Digital

Contact	Email	Responsibility
		Operational Queries
		Media/Press Enquiries
		Legal Issues
		Data Exchange Coordinator
		Security Incidents
		Freedom of Information requests

### Business as Usual Contacts – DH

Contact	Email	Responsibility
		Operational Queries
		Media/Press Enquiries
		Legal Issues
		Security Incidents

---

OFFICIAL

		Parliamentary Questions
		Freedom of Information requests

Escalation Contacts – Home Office

Contact	Email	Responsibility
Sonia Dower Director, Interventions & Sanctions Directorate	<a href="mailto:sonia.dower2@homeoffice.gsi.gov.uk">sonia.dower2@homeoffice.gsi.gov.uk</a>	Operational Queries
		Media/Press Enquiries
		Legal Issues
		Data Exchange Coordinator
		Security Incidents
		Parliamentary Questions
		Freedom of Information Requests

Escalation Contacts – NHS Digital

Contact	Email	Responsibility
		Operational Queries
		Legal Issues
		Data Exchange Coordinator
		Security Incidents
		Freedom of Information Requests

## Escalation Contacts – DH

<b>Contact</b>	<b>Email</b>	<b>Responsibility</b>
Gill Ayling Deputy Director, Digital & Technology Oversight	<a href="mailto:gillian.ayling@dh.gsi.gov.uk">gillian.ayling@dh.gsi.gov.uk</a>	Operational Queries
		Media/Press Enquiries
		Legal Issues
Lorraine Jackson Deputy Director, Data Sharing & Cyber Security	<a href="mailto:lorraine.jackson@dh.gsi.gov.uk">lorraine.jackson@dh.gsi.gov.uk</a>	Security Incidents
		Parliamentary Questions
		Freedom of Information Requests