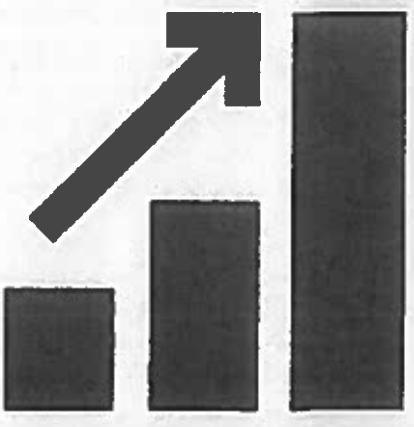
NHS England

Information Sharing Agreement - NHS England & Fire & Rescue Services in England



Information Sharing Agreement - NHS England & Individual Fire & Rescue Service in England.

National Health Applications and Infrastructure Services (NHAIS) Data

First published: 17th September 2015

Prepared by: Carol Mitchell – Head of Corporate IG

Classification: OFFICIAL

The National Health Service Commissioning Board was established on 1 October 2012 as an executive non-departmental public body. Since 1 April 2013, the National Health Service Commissioning Board has used the name NHS England for operational purposes.

Contents

	Information Sharing Agreement (where personal data is being processed)
1.	**Between:** NHS England and Each Fire & Rescue Service in England (see Annex A)
2.	**Definitions** See Annex B
3.	**Purpose & Objectives of the information sharing:** The Fire and Rescue Service (FRS) deliver Home Fire Safety Checks (HFSC) which has had a dramatic effect in reducing deaths and injuries in fires. Over 50% of these occur in households where over 65 year olds reside. Being able to specifically target this specific group will have an improved effect in reducing the risk of harm to those identified as well as reducing the impact on the NHS. As we have improved our ways of working, contact with older people will also lead to improved health and wellbeing by working with health and social care. This model of local working fits within the NHS vision of Vulnerability Hubs and adds significant capacity to community resilience. The sharing of this data is necessary for the FRS to exercise their duties and the data required cannot be obtained from another source e.g. the electoral role, as the data is not always accurate for over 65 age range as their residential status can be subject to more frequent changes. The Fire and Rescue Service (FRS) carry out around 670k home safety visits annually. As a result of joint work between NHS England, Public Health England, Local Government Association, Age UK and the Chief Fire Officers Association, these home safety visits are changing into 'safe and well' visits which aim to address a broader range of fire and health risks. This approach is set out in the Consensus Statement and Design Principles for Safe and Well Visits published in October 2015. **Objectives:** To reduce deaths and injuries as a result of fire or flood. To reduce the risk of harm to those identified and the subsequent impact on the NHS To enable the FRS to improve overall Health and Wellbeing by working closely with health and social care organisations. The further objective of this data sharing was to encourage local areas of the NHS to work with their local Fire and Rescue Service as part of the wider agenda for integrated care. This has already led to a broad range of approaches, often starting with shared health and fire risk factors such as falls, smoking, alcohol use. Risk factors are addressed through brief interventions and/or referrals to health/care/voluntary sector services.

4.	**Privacy Impact Assessment (PIA)** A privacy impact assessment has been undertaken as personal data is being processed The PIA has not identified any privacy concerns and it is recognised that there is processing of personal data. Although fair processing notices have been developed they do require strengthening. If this data was not shared the FRS would be still providing this service without the added value of being able to target the most at risk individuals, via a 'direct engagement' service and visiting every individual household. The address and year of birth of individuals is already data in the public domain; however the FRS cannot obtain an accurate dataset from the electoral role as the over 65 age range residential status can be subject to more frequent changes. The disclosure is in line with the NHS England's prevention agenda and the Caldicott Principle 7 – The duty to share information can be as important as the duty to protect patient confidentiality. The sharing of this data is in the best interest of the individuals. Assisting to reduce the cost and impact on critical healthcare services. Allows the FRS to prioritise and utilise their limited resources more effectively.
5.	**Legal basis and powers for processing the data/information**

Legislation	**Applicable to living individuals**	**Applicable to the deceased**
Vires/Legal powers to share NHS England Health & Social Care (Safety and Quality) Act 2015 (enacted October 2015) Inserts section 251B Duty to share information into the Health and Social Care Act 2012 Section 251B (3) requires NHS England (as a "relevant body" as defined in Section 251B) has a duty to share information where it is consider that disclosure is: a) likely to facilitate the provision to the individual of health services or adult social care in England; and b) in the individual's best interests. "Care" in this context is interpreted as consistent with NHS England's responsibilities in the prevention agenda and	**Yes**	***No***

	Vulnerability hubs The Health and Social Care Act 2012 Introduced legal duties on clinical commissioning groups and local authorities to have regard to the need for reduction of health inequalities and to exercise functions with a view to ensuring that services are provided in an integrated way where they consider that this would reduce inequalities in access to services and outcomes achieved. There is a strong relationship between vulnerabilities listed in the Chief Fire Officer Association (CFOA) Safe and Well toolkit and health inequalities. Therefore, reducing inequality by integrating the FRS Safe and Well visit is an important consideration for care providers and commissioners in providing services to prevent mortality and health problems. Fire and Rescue Services Act 2004, Section 6 – Fire Safety (1)A fire and rescue authority must make provision for the purpose of promoting fire safety in its area. (2)In making provision under subsection (1) a fire and rescue authority must in particular, to the extent that it considers it reasonable to do so, make arrangements for— (a)the provision of information, publicity and encouragement in respect of the steps to be taken to prevent fires and death or injury by fire; (b)the giving of advice, on request, about— (i)how to prevent fires and restrict their spread in buildings and other property; (ii)the means of escape from buildings and other property in case of fire. In line with the Fire and Rescue Services Act 2004 Section 11, Fire and Rescue services also have the following power which supports the Health and Wellbeing agenda set out in the Health and Social Care Act 2012: **11 Power to respond to other eventualities** (1) A fire and rescue authority may take any action it considers appropriate— (a) in response to an event or situation of a kind mentioned in			

	subsection (2); (b) for the purpose of enabling action to be taken in response to such an event or situation. (2) The event or situation is one that causes or is likely to cause— (a) one or more individuals to die, be injured or become ill; (b) harm to the environment (including the life and health of plants and animals). (3) The power conferred by subsection (1) includes power to secure the provision of equipment. (4) The power conferred by subsection (1) may be exercised by an authority outside as well as within the authority's area.			
	Data Protection Act 1998 – principle 1 NHS England has Fair Processing Information on its website which outlines how their data may be used and why it may be shared Fire & Rescue Services use a generic service-wide Fair Processing Notice, which can be found at Annex F		**Yes**	**No**
	Schedule 2 condition	5 (b) – see Schedule 2 (Annex D), bullet point 5 The processing is necessary for the exercise of any functions conferred by or under any enactment	**Yes**	**No**
	Schedule 3 condition	Not Applicable		
	Common Law duty of confidentiality Personal confidential data is not being shared with FRS, therefore common law duty of confidentiality does not apply in this instance.		**No**	**No**
	Human Rights Act 1998 - Article 8 **Is there any interference with Human Rights Article 8? –** There is an interference with HRA Article 8, but it is an interference which is permitted because it meets the requirements of HRA Article 8(2).		**Yes**	**No**
6.	**Data Controller(s)** NHS England Fire & Rescue Service in England			

7. Data items to be processed

Data Item(s)	Justification
Address Year of birth (pre 1950) Gender	FRS need to know which households to visit[1] To allow the FRS to prioritise resources to target those most at risk year of birth is required in order for the FRS to determine the age of the householder(s) because evidence they hold indicates that the older the householder, the higher the risk of harm or death from fire. The FRS requires gender because they have evidence which indicates that males are at a higher risk of harm or death from fires than females.

8. How will the processing be facilitated?

The data will be extracted from the Exeter system by NHS Digital previously known as the Health and Social Care Information Centre (HSCIC), acting as data processors on behalf of NHS England as the data controller. Data is sent via secure email to the individual Fire and Rescue Services ensuring that each service only receives data relevant to their geographical area.
In line with the FRS policy on Subject Access NHS England will facilitate any individual's objections where they are received however as the data is classified as non PCD, patient objections would not be applied by NHS Digital prior to dissemination unless a specific objection to the processing was made directly to NHS England.

9. Specify the procedures for dealing with DPA or FOIA access requests, or complaints or queries, from members of the public

See Box 13.

10. Specify the retention period for the information to be shared

2 years – The current calendar year for use, and 1 year for retention. The data will be destroyed confidentially and securely once the retention period is reached.

The Fire and Rescue services must provide NHS England with a certificate of data destruction to confirm permanent deletion of the data provided.

11. Specify the process for deleting/returning/safely destroying the information when it is no longer required (this should include provision for notification of such deletion/destruction)

See Box 10.

[1] Visits are applicable to any address where someone over 65 resides, even if there are people under 65 resident as well (although their details would not be released from NHAIS).

12.	**Specify any particular obligations on <u>all</u> parties to the agreement:** Each Fire and Rescue Service signed up to this Agreement will: 1. Use the information shared solely for the purposes identified and shall not access the information for any incompatible purpose. 2. Apply appropriate security measures, commensurate with the requirements of the 7th Data Protection Principle, which states that: "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". In particular, they shall ensure that measures are in place to do everything reasonable to: I. make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport II. deter deliberate compromise or opportunist attack, and III. promote discretion in order to avoid unauthorised access 3. Agree to treat the data received by them under the terms of this Agreement as confidential and shall safeguard it accordingly. Respect for the privacy of individuals will be afforded at all stages of carrying out the Purpose. For the avoidance of doubt, the obligations or the confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement. 4. Take appropriate organisational and technical measures towards compliance with Data Protection Act 1998, Caldicott, national information security management standards, Freedom of Information Act 2000 and national guidance and rules around processing personal information and other relevant legislation. 5. Commit to ensuring staff are appropriately trained and comply with organisational policies in relation to Information Governance, including data protection, confidentiality, Caldicott, Information Security, Records Management and Freedom of Information. 6. Promptly notify any other relevant co-signees of this agreement of any Information Governance breach resulting out of information shared under this Agreement. From June 2013 all Organisations processing health and adult social care personal data are required to use the IG Toolkit Incident Reporting Tool to report level 2 IG Serious Incidents Requiring Investigation (SIRIs) to the DH, ICO and other regulators. This requires an incident to be reported within 24 hours of it being identified and the same timeframe should be used for reporting to relevant partner signatories. NHS England will report any reported incidents via the IGT on behalf of the FRS. 7. Assist each other, in responding to Freedom of Information or Environmental Information Regulations requests where necessary, in relation to the information shared under this Agreement to ensure a co-ordinated and consistent response. 8. This Agreement shall be governed and construed in accordance with English Law and the parties agree to submit to the exclusive jurisdiction of the English Court. 9. Each Fire Service is to only get details of identifiable people applicable to their geographical area eg: Merseyside Fire and Rescue only get the details of over 65's who live in the Merseyside area. They do not get, or need, the details of over 65's living in Kent.
13.	**Specify any particular obligations on any individual party:** 1. NHS Digital to submit the data agreed above in a manner specified by the individual FRS. 2. The individual FRS's to report if the agreed information is not received, or if more information than required is delivered, to NHS England.

	3. The individual FRS's to handle any queries which arise regarding their need for the data and to investigate any incidents and report them within 2 days to the Corporate Information Governance team at NHS England –england.ig-corporate@nhs.net 4. If a local collaboration between a FRS and Health partners matures to the point where it is deemed that the FRS are collecting health data which is classified as sensitive under Schedule 3 of the Data Protection Act 1998, it is a requirement of NHS England that the FRS completes an annual IG Toolkit assessment or provides evidence that they hold ISO 27001 accreditation for Information Security Standards. 5. The FRS is specifically prohibited from any onward sharing of the data provided by NHS England unless permission has been sought and the sharing agreed. Should data be shared without agreement, this will render the FRS in breach of this agreement and may result in data no longer being provided. 6. NHS England agrees that the FRS can add a Unique Property Reference Number (UPRN) to the data provided to support their ability to clearly identify properties at risk of fire or flood. 7. FRSs may also use other data accessible such as; MOSAIC and internal data collated with the data subjects consent following previous referrals/visits to undertake a process of identifying those most at risk from severe harm or death. Where this combined data is used for a new purpose, the FRS should undertake a PIA to ensure that any privacy concerns are identified and managed appropriately. 8. Under the obligations of the Data Protection Act 1998 the FRS must provide data subjects with information about how their data is used and with whom it may be shared with. All FRS's receiving data from NHS England must therefore ensure that they can demonstrate that their fair processing information has been updated to reflect the new use of data.
14.	**Commencement of Agreement** 1st November 2016
15.	**Length of Agreement** The agreement will continue without end date however it will be reviewed and agreed by both parties on an annual basis.
16.	**Review of Agreement** A review of this information sharing agreement shall take place annually. All parties to this agreement agree to take part and fully cooperate in this review.
17.	**Term, termination and variation** a. Any Party may leave this Agreement by giving 60 days' notice in writing to the other Parties. b. Any proposed changes to the Parties involved in this Agreement, to the purposes of the information sharing, the nature or type of information shared or manner in which the information is to be processed and any other suggested changes to the terms of this Agreement must be notified immediately to the Information Compliance / Governance leads so that the impact of the proposed changes can be assessed. c. No variation of the Agreement shall be effective unless the agreement is amended and it

	is signed by all Parties.
18.	**Persons responsible for the development and review of this Agreement** Carol Mitchell – Head of Corporate IG, NHS England Carol.mitchell5@nhs.net
19.	**Dispute Resolution** In the event of a dispute arising under this Agreement, authorised representatives of the Parties will discuss and meet as appropriate to try to resolve the dispute within seven (7) days of being requested in writing by any Party to do so. If the dispute remains unsolved, it will then be referred to a senior manager from each of the Parties who will use all reasonable endeavours to resolve the dispute within a further fourteen (14) days. In the event of failure to resolve the dispute through the steps set out above the Parties agree to attempt to settle it by mediation.

NHS England & Fire and Rescue Services in England
Information Sharing Agreement
ISA v6.5 Oct 2016
Signatures

Signed for and on behalf of: NHS England *NB. specify service/area and include the address*	
Name:	Sir Bruce Keogh
Position:	NHS England Caldicott Guardian
Signature:	
Date:	3/11/16

Signed for and on behalf of **Name of Fire and Rescue Service:**	
Name:	
Position:	
Signature:	
Date:	

Annex A – List of Individual Fire & Rescue Services in England

FIRE & RESCUE SERVICE	Chief Fire Officers Name	Chief Fire Officer's Email Address	FRS website link to Fair Processing Notice
Avon			
Bedfordshire			
Buckinghamshire			
Cambridgeshire			
Cheshire			
Cleveland Fire Brigade			
Cornwall			
Cumbria			
Derbyshire			
Devon & Somerset			
Dorset and Wiltshire			
County Durham and Darlington			
Essex			
Gloucestershire			
Hampshire			
Hereford & Worcester			
Hertfordshire			
Humberside			
Isle of Wight			
Kent			
Lancashire			
Leicestershire			
Lincolnshire			

London Fire Brigade			
Manchester			
Merseyside			
Norfolk			
Northamptonshire			
Northumberland			
Northern Ireland			
Nottinghamshire			
Oxfordshire			
Royal Berkshire			
Shropshire			
Staffordshire			
Suffolk			
Surrey			
Sussex, East			
Sussex, West			
Tyne & Wear			
Warwickshire			
West Midlands Fire Service			
Yorkshire, North			
Yorkshire, South			
Yorkshire, West			

Annex B – Definitions

In this Agreement the following words have the following meanings:

Data Protection Act (DPA)	Means the Data Protection Act 1998 and any subsidiary or subordinate legislation as the same may be varied or replaced from time to time.
Data controller	as defined in the Data Protection Act 1998 – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are to be processed.
Data controllers 'in common'	Is where data controllers share a pool of personal data, each processing independently of the other.
Data processor	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. This means that the person processes data for a purpose and according to a manner determined by the data controller, and makes no independent determination of such matters.
Data Protection Principles	These are set out in Annex B attached to this Agreement and are required to be followed to ensure compliance with the DPA.
Data Subject	Data subject means an individual who is the subject of personal data.
'Fair' processing	All data controllers must have a Fair Processing Notice (otherwise known as a Privacy Notice), which is available to data subjects. A Fair Processing Notice is intended to make sure that data subjects are aware of how data is collected and used by the data controller. It aims to ensure that data controllers process personal data fairly and lawfully. Fair Processing Notices may be in oral or written form. The DPA sets out that, at a minimum, Fair Processing Notices should contain the following information - who the data controller is, what the data controller intends to do with their information and any other relevant information e.g. in the context of data sharing who the data will be shared with. Fair Processing Notices may also be used to provide additional information such as informing people about their subject access rights or the data controller's security arrangements.
"Joint" Data Controller	"Joint" covers the situation where the determination is exercised by data controllers acting together, typically with written agreements setting out the purposes for processing, the manner of processing and the means by which joint data controller responsibilities will be satisfied. All must have the authority to determine or prevent data processing, i.e. that they are consulted is insufficient to qualify them as a data controller.
Personal data	Personal data means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, 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.
Privacy impact assessment (PIA)	A privacy impact assessment (PIA) is a process that focuses on identifying the impacts on privacy of any new project, technology, service or programme and, in consultation with stakeholders, taking remedial actions to avoid or mitigate any risks.
Processing	Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:–
Sensitive data	Means 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 (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

Annex C – Data Protection Principles

The Data Protection Act 1998 applies to living individuals and gives those individuals a number of important rights to ensure that personal information covered by the Act is processed lawfully. It regulates the manner in which such information can be collected, used and stored, and so is of prime importance in the context of information sharing. Key principles in the DPA that are relevant to information sharing are:

The DPA's eight data protection principles

1st principle Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

(a) at least one of the conditions in Schedule 2 is met,
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2nd principle Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3rd principle Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4th principle Personal data shall be accurate and, where necessary, kept up to date.

5th principle Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6th principle Personal data shall be processed in accordance with the rights of data subjects under the DPA.

7th principle Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8th principle Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Annex D – Conditions for Processing

To enable a Data Controller to release data it holds, a condition for processing must be satisfied. These are outlined below.

To release personal data (as defined by the Data Protection Act), a Schedule 2 condition must be met. Where ***sensitive*** personal data is to be released, then a condition from both Schedule 2 **and** Schedule 3 must be satisfied.

Schedule 2	Schedule 3
• The individual who the personal data is about has consented to the processing. • The processing is necessary: - in relation to a contract which the individual has entered into; or - because the individual has asked for something to be done so they can enter into a contract. • The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract). • The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident. • The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions. • The processing is in accordance with the "legitimate interests" condition*. * *The Data Protection Act recognises that you may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided you meet certain requirements.* *The first requirement is that you must need to process the information for the purposes of your legitimate interests or for those of a third party to whom you disclose it.* *The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. Your legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.*	• The individual who the sensitive personal data is about has given explicit consent to the processing. • The processing is necessary so that you can comply with employment law. • The processing is necessary to protect the vital interests of: - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or - another person (in a case where the individual's consent has been unreasonably withheld). • The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition. • The individual has deliberately made the information public. • The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights. • The processing is necessary for administering justice, or for exercising statutory or governmental functions. • The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality. • The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals. *In addition to the above conditions – which are all set out in the Data Protection Act itself – regulations set out several other conditions for processing sensitive personal data. Their effect is to permit the processing of sensitive personal data for a range of other purposes – typically those that are in the substantial public interest, and which must necessarily be carried out without the explicit consent of the individual. Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration. A full list of the additional conditions for processing is set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders.*

Many of the conditions for processing depend on the processing being "necessary" for the particular purpose to which the condition relates. This imposes a strict requirement, because the condition will not be met if the organisation can achieve the purpose by some other reasonable means or if the processing is necessary only because the organisation has decided to operate its business in a particular way.

What is meant by "consent"?

One of the conditions for processing is that the individual has consented to their personal data being collected and used in the manner and for the purposes in question.

You will need to examine the circumstances of each case to decide whether consent has been given. In some cases this will be obvious, but in others the particular circumstances will need to be examined closely to decide whether they amount to an adequate consent.

Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual's consent as:

"...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

The fact that an individual must "signify" their agreement means that there must be some active communication between the parties. An individual may "signify" agreement other than in writing, but organisations should not infer consent if an individual does not respond to a communication – for example, from a customer's failure to return a form or respond to a leaflet.

Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. For example, if your organisation intends to continue to hold or use personal data after the relationship with the individual ends, then the consent should cover this. Even when consent has been given, it will not necessarily last forever. Although in most cases consent will last for as long as the processing to which it relates continues, you should recognise that the individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in which you are collecting or using the information. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given.

You should review whether a consent you have been given remains adequate as your organisation's relationship with an individual develops, or as the individual's circumstances change.

Consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

The Data Protection Act distinguishes between:

- the nature of the consent required to satisfy the first condition for processing; and
- the nature of the consent required to satisfy the condition for processing sensitive personal data, which must be "explicit".

This suggests that the individual's consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the

purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

As explained above, a particular consent may not be adequate to satisfy the condition for processing (especially if the individual might have had no real choice about giving it), and even a valid consent may be withdrawn in some circumstances. For these reasons an organisation should not rely exclusively on consent to legitimise its processing. In our view (*the ICO*) it is better to concentrate on making sure that you treat individuals fairly rather than on obtaining consent in isolation. Consent is the first in the list of conditions for processing set out in the Act, but each condition provides an equally valid basis for processing personal data.

Annex E – Applicable Legislation

Applicable legislation[2]

1. There is no single source of law that regulates the powers that a public body has to use and to share personal information. The collection, use and disclosure of personal information is governed by a number of different areas of law as follows:
    - the law that governs the actions of public bodies (administrative law);
    - the Data Protection Act 1998
    - the Human Rights Act 1998 and the European Convention on Human Rights;
    - the common law tort of breach of confidence;

2. The interrelationship between the above areas of law is quite complex. The starting point is always to determine whether the public body has the power to carry out any proposed data sharing. This will be a matter of administrative law.

3. **Administrative law** governs the actions of public authorities. According to well established rules, a public authority must possess the power to carry out what it intends to do. If not, its action is *ultra vires*, i.e. beyond its lawful powers. It is also necessary that the power is exercised for the purpose for which it was created or is 'reasonably incidental' to the defined purpose. It is important that all NHS bodies are aware of the extent and limitations of their powers and act *intra vires* (i.e. within their lawful powers). The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the *ultra vires* rule) is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function. However, unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place, for example by obtaining explicit patient consent.

Data Protection Act 1998

Common Law Duty of Confidentiality [3]

4. Data sharing will not be 'lawful' for the purposes of the first data protection principle (or 'in accordance with the law' for the purposes of Article 8 of the ECHR) if it involves a breach of confidence. The common law, case law determined by the Courts, has established that information provided by individuals in confidence should generally be protected and not disclosed to anyone other than the person to whom the information was provided or used for other purposes without their consent. The duty of confidentiality owed by clinicians to their patients is well established and is in addition to the requirements of the Data Protection Act 1998 and other legislative requirements.

---

[2] http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf
https://www.gov.uk/government/publications/nhs-information-governance-legal-and-professional-obligations

[3] National Information Governance Board (NIGB) - Identifying and contacting patients for medical research – summary of the legal framework

5. For the common law duty of confidentiality to apply the information must be confidential in nature or imparted with an expectation of confidentiality. Normally information already in the public domain would not be regarded as having the necessary quality of confidentiality, however sometimes demographic data can be sensitive or imparted with an expectation of confidentiality and caution should be exercised in such cases.

6. The common law provides protection for confidential patient information in particular because of the importance confidentiality plays in the clinical relationship, allowing patients to divulge sensitive information without concern that it will be disclosed to others.

7. Maintaining public trust in a confidential service is therefore in the public interest and is strongly supported by the courts. As with the Data Protection Act, information that has been anonymised is exempt.

8. Other exemptions from the common law duty of confidence may apply when:

    - The law requires or permits disclosure through statute or court order.
    - There is a public interest necessitating disclosure which is sufficient to outweigh both the private interests of the individual and the public interest in maintaining public trust in a confidential service.

Section 251

9. Section 60 of the Health and Social Care Act 2001 as re-enacted by Section 251of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes.

10. The Regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. Any references to 'section 251 support or approval' actually refer to approval given under the authority of the Regulations.

11. Section 251 was established to enable the common law duty of confidentiality to be overridden to enable disclosure of confidential patient information for medical purposes, where it was not possible to use anonymised information and where seeking consent was not practical, having regard to the cost and technology available.

The NHS Care Record Guarantee

12. The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to patients' rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant in relation to this policy is:

    Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

    - You ask us to do so.
    - We ask and you give us specific permission.
    - We have to do this by law.
    - We have special permission for health or research purposes; or
    - We have special permission because the public good is thought to be of greater importance than your confidentiality, and

- If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of Practice and other national guidelines on best practice.

Human Rights Act 1998 and the European Convention on Human Rights

13. Data sharing by public authorities must comply with the European Convention of Human Rights (now part of the UK domestic law as a result of the **Human Rights Act 1998**), and in particular Article 8, which provides:

    Everyone has the right to respect for his private and family life, his home and his correspondence.
    There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

14. Processing personal data (including sharing it) will often constitute an 'interference' with the right to respect for private and family life within the meaning of Article 8. However, an interference will be compatible with Article 8 if it meets the requirements of Article 8(2).

15. The interference must be 'in accordance with the law: it must have a proper basis in national law and that law must be adequately accessible and foreseeable.

16. If a public body has a lawful basis for sharing data, as set out in section 3 above, then it is likely that this requirement will be met.

17. The interference must answer a 'pressing social need', which will be the case if it pursues a legitimate aim in a proportionate manner and is accompanied by appropriate safeguards.

Annex F – Fair Processing Notices

Below is the Fair Processing Statement used by each FRS in England.

NHS England, the Royal College General Practitioners and Fire and Rescue Services (FRS) in England work together to ensure preventative resources are offered to those who may benefit most. This is achieved by referrals and the sharing of information (where relevant, proportionate and necessary) to allow fire service personnel to undertake Safe and Well visits. If you require more information about how NHS England use and share your information, please click on the following link: https://www.england.nhs.uk/contact-us/privacy-notice/your-information/

Research has shown that those at high risk from fire death and injury are those who are most likely to impact on a range of NHS services. Safe and well visits are developed between local health practitioners and FRSs to meet local health-risk priorities. They therefore represent an intervention which can improve people's quality of life while reducing demand on critical services.

The majority of fire deaths in the UK occur amongst the elderly population. However older people are most vulnerable to fire and a number of other risks. A Safe and Well visit from the FRS is proven to make them safer and can reduce risk significantly across a range of factors.

In one area of the United Kingdom where this work has been piloted since 2007, there has been a very significant reduction in fire deaths and injuries which has developed into a current trend well below the national average. So we know this work can save many lives.

The FRS and NHS will continue to work together in the future to ensure the visits undertaken by the FRS are effective in helping to make making people safe and well.

NHS England has also developed a Fair Processing Notice for this purpose:

NHS England is Data Controller for the National Health Applications and Infrastructure Services (NHAIS) system. This system holds demographic details of all patients registered with GP in England and Wales. There are also links to similar systems in Scotland, IoM, and Northern Ireland.

The NHAIS systems have been in operation since the early 1980's and from the creation of the original Exeter database, a facility referred to as 'Open Exeter' was then developed for the NHS 50th Exhibition in July 1998 and referred to in the white paper 'An Information Strategy for the Modern NHS 1998 – 2005'.

NHAIS systems form one of the largest databases in operation in England and were previously managed by Connecting for Health and latterly NHS Digital (formerly known as the Health and Social Care Information Centre (HSCIC)). Under the revised GMS contract regulations, NHS England is responsible for maintaining a list of patients registered with GP contractors in England. This data comprises of demographic data only and does not include any clinical information relating to patients. NHS England is the primary data controller for the core registration data within NHAIS.

Although information from the core Exeter database also feeds into subsidiary systems in Wales, Northern Ireland, and the Isle of Man, NHS England are only responsible for the core data processed within England. The NHAIS Registration system now manages in excess of 60 million records; it forms the core of an extensive primary care management base centred on a computerised index of NHS patients.

The information held in these systems is primarily used for healthcare purposes, but may also be used for other non-healthcare related purposes, and shared with other statutory bodies/organisations to enable them to fulfil their statutory obligations.

The information will only be shared with other organisations where there is a statutory obligation to do so, or with the agreement of NHS England's Caldicott Guardian.

For more information, please contact NHS England's Corporate Information Governance Team:england.ig-corporate@nhs.net