Dr Foster Unit at Imperial College (DFU) – Privacy Notice

What is the purpose of this document?

Imperial College of Science, Technology and Medicine (the "**College**" or "**Imperial**") is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your relationship with us, in accordance with the applicable data protection legislation (the Data Protection Act 2018, the General Data Protection Regulations (the "**GDPR**") and the College's *Data Protection Policy*.

The College is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to members of the public. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We may collect, store, and use the following categories of personal information about you. These categories are stored and processed separately from the special categories contained in research data and are used by care providers for patients under their care:

- NHS Number.
- Local patient identifier – a number used to identify a patient within a health care provider (e.g. an individual patient's hospital number).

We may also collect, store and use the following "special categories" of more sensitive personal information as anonymous / de-identified data. These data are stored and processed separately to the identifiable data:

- Information about your race or ethnicity.
- Information about your health, including any medical condition, health and sickness records.

How is your personal information collected?

We collect the personal information about you by agreement with NHS Digital using their Secure Electronic File Transfer service (SEFT). DFU meets strict governance standards in order to complete NHS Digital's Data Access Request Service (DARS) agreements.

How we will use information about you and the legal basis for processing your data under the GDPR

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to comply with a legal obligation.

2. Where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

4. Where it is necessary in order to protect your vital interests or someone else's vital interests.

Situations in which we will use your personal information

We need all the categories of information in the list above (see The kind of information we hold about you) primarily to help NHS organisations improve the standards of care patients receive. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Analysing the de-identified information to highlight variations in the quality of patient care.
- Helping the NHS drive up standards by using de-identified hospital information to spot when hospitals have higher than expected mortality rates.
- Improving care by using the de-identified data in research to find the best ways to measure quality of care and to compare hospital treatments.

- Alerting NHS organisations of potential problems with quality and safety of care. The identifiable information is used by hospitals to retrieve their own clinical records for further investigation.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Change of purpose

We will only use your personal information for the purposes agreed with NHS Digital in our DARS agreements. If we need to use your personal information for an unrelated purpose, NHS Digital will first have to approve new or amended DARS agreements.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where it is necessary in the context of employment law, or laws relating to social security and social protection.

3. Where the processing is necessary to protect your vital interests (or those of another person) where you are incapable of giving consent.

4. Where the processing is carried out in the course of our legitimate activities as a charity, with respect to our own members, former members, or persons with whom we have regular contact in connection with our purposes.

5. Where the processing relates to personal data which have been manifestly made public by you.

6. Where the processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity.

7. Where the processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects your rights as a data subject.

8. Where the processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and services.

9. Where the processing is necessary for reasons of public interest in the area of public health (e.g. ensuring the safety of medicinal products).

10. Where the processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards.

Our obligations

We will use your particularly sensitive personal information in the following ways as de-identified data:

- Analysing the de-identified information to highlight variations in the quality of patient care.
- Helping the NHS drive up standards by using de-identified hospital information to spot when hospitals have higher than expected mortality rates.
- Improving care by using the de-identified data in research to find the best ways to measure quality of care and to compare hospital treatments.

Do we need your consent?

Patient objections have been applied and opt out upheld for data made available under Section 251 for the admitted patient care (APC) data and critical care (CC) data that we receive. Opt outs do not apply to accident and emergency (AE) data or outpatient (OP) data as no identifiable data are provided.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.

2. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the College group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We are not permitted to transfer the de-identified or identifiable information outside the EU.

Why might you share my personal information with third parties?

We may share your personal information with third parties where required by law, where it is necessary to administer the relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within the College group. The following third-party service providers process de-identified personal information about you for the following purposes:

- Dr Foster Limited – to provide products or services using the de-identified data only to public bodies including: The National Health Service, The Care Quality Commission, The NHS Trust Development Authority, Department of Health, Public health England. Dr Foster Limited provides a range of information systems to help clinicians and managers to better understand their performance and safety in context of others. This is under sub-licence, approved by NHS Digital.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the College group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business and operations of the College. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Data security

We have put in place measures to protect the security of your information. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. All data will be destroyed once their retention period has been met, and when the unit has made the decision that the data are no longer required. We destroy all patient identifiable information from our records which are older than three years.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the College's Data Protection Officer in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the College's Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Officer

We have appointed a Data Protection Officer to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Officer at:

Imperial College London
Data Protection Officer
Exhibition Road
Faculty Building Level 4
London SW7 2AZ

e-mail: *dpo@imperial.ac.uk*

If you require access to your health records stored by DFU you must make a written request to:

Professor Paul Aylin
Co-Director Dr Foster Unit
School of Public Health
Imperial College London 3 Dorset Rise
London
EC4Y 8EN

Telephone: +44 (0)20 7594 3334
Email: p.aylin@imperial.ac.uk

If you have a concern about the way your records are managed or to learn more about how DFU use, manage and maintain confidentiality of your information, please contact:

Anthony Thomas
Data Manager
Dr Foster Unit
School of Public Health
Imperial College London

3 Dorset Rise
London EC4Y 8EN

Telephone: +44 (0)20 7332 8962
Email: anthony.thomas@imperial.ac.uk

You have the right to make a complaint at any time to the Information Commissioner's Office (**ICO**), the UK supervisory authority for data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.