NHS
University Health Service

Staff Privacy Information Form

The General Data Protection Regulations are enforceable from the 25th May 2018. These regulations require University Health Service ("The Practice") to provide information to its employees on what personal data is held and/or processed, the purpose for which the data is being processed and how long the data will be stored. Employees have the legal right to make a Subject Access Request to rectify or delete their personal data.

This Privacy Information Form is designed to explain all of the above to you, as well as to provide robust information to enable you to feel confident in The Practice's processes. Please read the details contained within this form carefully as it sets out how we, as the Data Controller will work with you and any internal and external Data Processors to your data is kept secure. Once you have read and understood this form, please sign to confirm your understanding.

If you require any further information or guidance, or have any questions on the details contained within this form, please seek immediate advice from the practice manager. Alternatively, you can access the following resources (among others available on the internet):

- ACAS - Guide to Data Protection: http://www.acas.org.uk/index.aspx?articleid=3717
- Information Commissioner's Office - Guide to GDPR: https://ico.org.uk/your-data-matters/
- xPertHR - Guide to GDPR: https://www.xperthr.co.uk/faq/what-information-must-employers-supply-to-employees-about-the-processing-of-their-personal-data-under-the-general-data-protection-regulation-gdpr-/162313/

1. Definition of Key Terms within the GDPR

For the purposes of this form, the GDPR provides the following definitions:

Data Subject (you*)*
"The individual who is the subject of personal data."

Personal Data
"Any information relating to an identified or identifiable natural person… such as name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Personal data must not be irrelevant or excessive with regards to the Agreed Purposes set out in Section 5.

Sensitive Personal Data
"Means personal data consisting of information such as:- the racial or ethnic origin of the data subject, political opinions, religious or other beliefs, physical or mental health or condition, data relating to sex life, criminal record or member of Trade Union."

Consent
"[Being] freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Controller (The Practice)
The [person or company] which, alone or jointly with others, determines the purpose and means of the processing of personal data."

Processor
The [person or company] which processes personal data on behalf of the Controller.

Processing
"Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organising, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, erasure or destruction."

Personal Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." This includes: access by an unauthorised third party, deliberate or accidental action (or inaction) by the controller or processor, sending personal data to an incorrect person or for example, computing processing devices being lost or stolen.

Other definitions are available from the Information Commissioners Office (ICO).

2. **Consent**
Consent features heavily within the GDPR and basically means that you need to give your 'consent' to us to enable us to hold and process your personal data. The Regulations state that consent must be freely given, specific, informed and unambiguous. Under your employment contract, there are certain areas that you will need to consent to as it is in your interest to do so, for example, we will need your bank account details to enable us to process your salary! However, please be aware that you are within your rights to withdraw your consent at any time, in writing.

3. What information will we hold about you and why?
For the purpose of this form, The Practice as the Data Controller require the following personal information from you for the reasons noted alongside. Personal data will not be used for any other purpose without the written authority of the Data Controller.

What Personal Data is Required	Purpose
Name DOB Address NI number Passport information	Payroll & pension processing Compliance to work in UK
Next of kin details Driving licence CPD information Annual leave and sickness records Disciplinary and Grievance records	In case of accident To ensure ID and address Required for compliance Payroll, staff information and compliance with DWP HR reviews and performance issues

The Practice will hold the above information for the duration of your employment with us. However, it will be reviewed on an annual basis for 1) currency, 2) validity and 3) to ensure you are still happy to provide your consent.

4. Who might we share your information with?

Your personal information is collected specifically for the areas raised in Section 3 above, however, there are times when we do have to share your personal data – for the purpose of transparency, these are noted below:

Name of External Company	Purpose
HMRC	Payroll Processing
NHS Pension Scheme	Uploading of pension contributions
NatWest Bank	Payroll processing

5. What we do with your information.

The information that you provide us with is stored within the practice server. The server profile storing this data is only accessible via a unique password. Your details are scanned and stored on here for the duration of your employment with us for employment compliance purposes. Personal data is only available to the practice manager and the partners.

6. How long do we hold your information?

For practice purposes: For the whole time you are employed by The Practice.
For HMRC's purposes: 5 years.
For NHS Pension Authority purposes: 3 years

7. How can you access information we hold about you?

Data Subjects (you) have the right to access the personal data we hold about you – this is called a Subject Access Requests . Under the GDPR, you have the following 8 rights:

(i) The right to be informed
(ii) The right of access
(iii) The right to rectification
(iv) The right to erasure
(v) The right to restrict processing
(vi) The right to data portability
(vii) The right to object
(viii) Rights in relation to automated decision making and profiling

To make a SAR, you are advised to contact the practice manager stating what specific information you would like to access, which we will provide in electronic format. We aim to provide any data following an access request within one month. With your SAR, you will need to provide us with the following information:

- Your full name, address, contact telephone number and email address
- Details of the specific information you require and any relevant dates.

We are able to provide your SAR to third parties providing we have a written instruction from you to confirm your agreement for us to share any information held, for example, you may wish to take out a critical illness cover, and the third party will need to confirm your employment status with us.

8. Making a Complaint

We sincerely hope that there is never an occasion for our employees to have to resort to making a complaint regarding information security, however, we appreciate that at times things go wrong. In the unfortunate situation that this happens, please book a meeting with the practice manager.

Alternatively, you have the right to complain direct to The Practice's Data Protection Officer:
DPO: Dr Ali Robins
By post: SPCL, Sovereign Place, Upper Northam Road, Hedge End, Southampton, SO30 4BZ
By email: spcl.dpo@nhs.net

Our written complaints procedure is available upon request. If we cannot settle your complaint, you may be entitled to refer it to the Information Commissioner's Office (ICO) – further information is available from their website www.ico.org.uk/concerns/ or by telephone on 0303 123 1113.

9. Confirmation of Agreement

I confirm that I have read this Privacy Information Form and understand what personal data is being collected about me, the purpose of this, as well as storage and security measures, under the General Data Protection Regulations.

Signed: _____ Date: _____

Name: _____

I confirm that I give my consent freely for the areas listed in section 3.

Signed: _____ Date: _____

Name: _____

University Health Service
Building 48
University of Southampton
Highfield
Southampton SO17 1BJ

Tel: 023 8055 7531
Email: surgery@unidocs.co.uk

VERSION HISTORY			
Version	Date	Author	Notes
1	13/5/18	SPCL	
2	6/6/18	ME	