**UK GDPR Privacy Notice**

**Guidance Notes**

A core requirement of the UK GDPR is that your privacy notice needs to be ‘accessible’ to your data subjects. The easiest way to ensure your privacy notice is ‘accessible’ is by publishing it on your own profile page on your affiliated hospital/ surgery website.

Furthermore, it is ***essential***that your privacy notice is genuinely reflective of your own practice. While your practice may be similar to that of your medical colleagues, you are all likely to manage and store information differently and therefore your own circumstances, and as such your privacy notice, should be unique to you.

The following template can be adapted to your own needs by inserting relevant details where required at [x], by deleting any information that does not apply to you, and amending any terminology not used within your practice.

If you have drafted a privacy notice or notice previously, you do not need to complete a new one; you can simply review your existing notice and update it with any changes that may have occurred since it was last reviewed.

**PRIVACY NOTICE OF:**

**[INSERT BUSINESS NAME OF HEALTHCARE PROFESSIONAL]**

**[INSERT BUSINESS ADDRESS]**

**[INSERT ICO REGISTRATION NUMBER]**

**[INSERT DATE]**

**Notice became operational on: [1 January 2023]**

**Next review date: [1 January 2024]**

**Privacy Notice**

*In order to provide medical advice and treatment, I need to collect and hold personal information. This may be your personal data or information relating to other patients. I will take all possible steps to protect personal information. I will ensure that I do not do anything that may infringe your rights or undermine your trust. This privacy notice describes the information I collect about you, how it is used and shared, and your rights regarding it.*

***Data controller***

*I, [Insert name], I am registered with the Information Commissioner’s Office (ICO) as a Data Controller for the personal data that I hold and process as a medical professional. My registered address is [x] and my ICO registration number is [x]. If you need to contact me about your data or this privacy notice, you can reach me at [insert email address].*

***Data collection***

*[All] or [The vast majority] of the information that I hold about you is provided to, or gathered by, me in the course of providing you with medical advice or treatment. I will tell you why I need the information and how I will use it. In addition to the information you may provide to me, I also obtain information from other sources as follows:*

* *Your General Practitioner (GP)*
* *Other medical professionals; both private and public professionals;*
* *Information received from Northern Ireland Health and Social Care Trusts*
* *All Healthcare results such as X-ray, CT or MRI results, blood tests etc.*
* *Information received from other people who may care for you such as relatives*
* *Legal professionals including solicitors and barristers and their associates, trainees and staff for the purpose of providing any medical expert reports*
* *Regulatory, public or administrative bodies*

**What data do I process about you?**

Depending on the type of work, I collect and process both personal data and special categories of personal data as defined in the UK GDPR. This may include:

* Name
* Email address
* Phone number
* Address
	+ Medical insurance details, including membership numbers and compensation history
* Payment or bank details
* Date of birth
* Next of kin details
	+ Details employment Information on your background & current circumstances
* INSERT ANY OTHER TYPES OF INFORMATION YOU PROCESS

Where relevant, I may also need to process special category personal data that reveals your:

* Genetic data
* Biometric data for the purpose of uniquely identifying a natural person
	+ Data concerning health, including medical reports and results from other healthcare professionals and organisations
* Sex life and sexual orientation
* Racial or ethnic origin
* Religious and philosophical beliefs

**My lawful basis for processing your information**

In order that I can provide medical services and advice to you, I must process your personal data. The UK General Data Protection Regulation (the UK GDPR) requires that where I process personal data, I must have a lawful basis for doing so. The lawful bases identified in the UK GDPR that I seek to rely upon are as follows:

* **Consent of the data subject**–where this required, I will ensure that I have your specific consent for processing your data for the specified purposes. You will also have the right to withdraw your consent at any time. Where you do so this will not affect the legality of data processing which had taken place prior to your withdrawal of consent.
* **Performance of a contract with the data subject, or to take steps to enter into a contract.**
* **Compliance with a legal obligation**–to comply with various regulatory and professional obligations, e.g. General Medical Council (GMC) and for filing tax returns with HMRC.
* **To protect the vital interests a data subject or another person;**
* **The legitimate interests of my business or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.**

Examples of legitimate interests include but are not limited to:

* Where the data subject is a client or in the service of the controller
	+ Transmission within a group of undertakings for internal administrative purposes
* For completion of professional regulatory requirement
* Processing for direct marketing purposes, or to prevent fraud
* Reporting threats to public security
* Such other purposes as set out below

**Special category processing**

The UK GDPR specifies that where I process special category data, I must rely upon certain exemptions in order to do so lawfully. The following exemptions are applicable in my practice

1. I have your explicit consent to do so; or
2. It is necessary for the exercise or defence of legal claims or judicial acts.

**Purposes:**

**I use your personal information for the following purposes:**

* Provide medical advice and treatment;
* Assist in training staff;
* Investigate and address your concerns;
	+ To work effectively with other medical professionals and organisations who may be involved in your medical care, such as the Health and Social care Trust.
	+ For reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, such as the Covid-19 virus,
	+ Investigate or address legal proceedings relating to your use of my services, or as otherwise allowed by applicable law;
* To comply with GMC
* Make statutory returns as required by HMRC
* For marketing purposes.
* For the management and administration of my practice
* For Research and Audit purposes
* [OTHER USES TO BE INSERTED AS APPROPRIATE]

**In the course of processing your information to provide medical services to you, I may share your personal data with:**

* Referring doctors/organisations
* Staff under my training
* My office management and staff who provide administrative services for my practice
* My regulator or legal advisors in the event of a dispute, complaint or other legal matter
* Law enforcement officials, government authorities, or other third parties, to meet any legal obligations
* Any other party where I ask you for consent, and you consent, to the sharing
* [INSERT MORE AS APPROPRIATE]
	+ I may also be required to disclose your information to the Police or Intelligence services where required by law or pursuant to a court order

**Transfers to third countries and international organisations**

[I do not transfer any personal data to third countries or international organisations outside of the UK.]

OR

[I transfer personal data outside of the UK to the following third countries (including all EEA states) or international organisations using the identified safeguards because INSERT PURPOSE FOR DOING SO.]

1. INSERT COUNTRY AND TRANSFER SAFEGUARD IN PLACE

[In addition, I may process personal data pertaining to data subjects outside of the UK, such as EEA citizens. Where this is the case, I am satisfied that such transferred data is fully protected and safeguarded as required by the UK- General Data Protection Regulation and the EU- General Data Protection Regulation.]

**I retain your personal data** while you remain a [patient] unless you ask me to delete it. My Retention and Disposal Notice (copy available on request) details how long I hold data for and how I dispose of it when it no longer needs to be held. I will delete or anonymise your information at your request unless:

* There is an unresolved issue, such as a claim or dispute;
* I am legally required to; or
* There are overriding legitimate business interests to do so.

**Your rights**

The UK GDPR gives you specific rights in terms of your personal data. For example, you have the right of access to the information I hold and what I use it for;

you can ask for a copy of the personal information I hold about you.

You can ask me to correct any inaccuracies with the personal data I hold, and you can ask me to stop sending you direct mail or emails or, in some circumstances, ask me to stop processing your details.

Finally, if I do something irregular or improper with your personal data, you can complain to the ICO if you are unhappy with how I have processed your information or dealt with your query. You may also seek compensation for any distress you are caused or loss you have incurred.

You can find out more information from the ICO’s website:

<http://ico.org.uk/for_the_public/personal_information>

**Accessing and correcting your information**

You may request access to, correction of, or a copy of your information by contacting me at [x email address].

**Marketing opt-outs**

You may opt out of receiving emails and other messages from my practice by following the instructions in those messages.

**I will occasionally update my privacy notice.** When I make significant changes, I will notify you of these [through either mail or email [OR INSERT ALTERNATIVE]]. I will also publish the updated notice on [my website/practice’s website profile].