

---

# Privacy Notice Explained

## What is a Privacy Notice?

A Privacy Notice (or 'Fair Processing Notice') is an explanation of what information the Practice collects on patients, and how it is used. Being transparent and providing clear information to patients about how a Practice uses their personal data is an essential requirement of the Data Protection Act 1998.

Under the DPA, the first principle is to process personal data in a fair and lawful manner, and applies to everything that is done with patient's personal information. In practice, this means that the Practice must;

- ✓ have legitimate reasons for the use or collection of personal data
- ✓ not use the data in a way that may cause adverse effects on the individuals (e.g. improper sharing of their information with 3<sup>rd</sup> parties)
- ✓ be transparent about how you the data will be used, and give appropriate privacy notices when collecting their personal data
- ✓ handle personal data only as reasonably expected to do so
- ✓ make no unlawful use of the collected data

## Fair Processing

Personal data must be processed in a fair manner – the DPA says that information should be treated as being obtained fairly if it is provided by a person who is legally authorised or required to provide it. Fair Processing means that the Practice has to be clear and open with people about how their information is used.

Providing a 'Privacy Notice' is a way of stating the Practice's commitment to being transparent and is a part of fair processing, however you also need to consider the effects of processing on the individuals and patients concerned;

- ✓ What information are we collecting?
- ✓ Who collects the data?
- ✓ How is it collected?
- ✓ Why do we collect it?
- ✓ How will we use the data?
- ✓ Who will we share it with?
- ✓ What is the effect on the individuals?
- ✓ If we use it as intended, will it cause individuals to object or complain?

Conducting a Privacy Impact Assessment is an effective way of assessing whether you can safely collect or use patient data according to the DPA and Information Governance requirements. The Information Commissioners' Office has published guidance on carrying out a PIA and can be found here:

<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

## Data Controllers

Under the Data Protection Act, the data controller is the person or organisation that will decide the purpose and the manner in which any personal data will be processed – they have overall control of the data they collect, and decide how

and why it will be processed.

A GP Practice is a data controller for the patient information it collects, and should already have data processing arrangements with third parties (e.g. IT systems providers) to ensure they do not use or access data unlawfully; the data controllers will have ultimate responsibility for the Practices' compliance with the DPA.

## **Risk Stratification**

This is a process to identify and manage patients that are more likely to need secondary care – information is collected in order to assess their 'Risk Score' and is sent to NHS organisations to assess and return the results to the GP Practice. This is an acceptable way of assessing patients' needs and prevent ill health, however it is also regarded as a disclosure of personal information, and patients have the option to opt out of any data collection at the Practice, and needs to be made clear to them.

## **Invoice Validations**

If a patient has had NHS treatment, their personal information may be shared within a secure and confidential environment to determine which CCG should pay for the treatment received. This means sharing identifiable information such as name, address, date of treatment etc. to enable the billing process.

## **Partner Organisations**

If the Practice shares information with any external organisations (within or outside the NHS), then let patients know by listing them. Partner organisations will usually include NHS organisations (hospitals, CCGs, NHS England etc.) other public sectors (Education, Police, Fire etc.) and any other Data Processors that may be carrying out specific project work with the Practice (e.g. Diabetes UK).

## **Access to Personal Information**

The DPA gives patients the right to view any information held about them – the 'Right of Subject Access'. Explain the process and who to contact. You can find your practice registration number by entering your Practice name in the 'Name' box here; <https://ico.org.uk/ESDWebPages/Search>