

# Sharing and accessing electronic patient records



Version:	Review date:	Edited by:	Approved by:	Comments:
1	December 2019	Emily Dewey	Dr Ku Rama	

## Table of contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Policy statement	2
1.2	Status	2
1.3	Training and support	2
<b>2</b>	<b>Scope</b>	<b>2</b>
2.1	Who it applies to	2
2.2	Why and how it applies to them	2
<b>3</b>	<b>Definition of terms</b>	<b>2</b>
3.1	Department of Health and Social Care	2
3.2	Royal College of General Practitioners	3
3.3	British Medical Association	3
3.4	General Data Protection Regulation	3
3.5	Explicit consent	3
3.6	Confidentiality	3
3.7	Information sharing	3
<b>4</b>	<b>Policy</b>	<b>4</b>
4.1	Sharing agreements	4
4.2	Legitimate relationships	4
4.3	Access controls	4
4.4	Privacy	4
4.5	Consent	5
4.6	Restrictions	5
4.7	System specifics	5
<b>5</b>	<b>Summary</b>	<b>6</b>

# 1 Introduction

---

## 1.1 Policy statement

The Department of Health and Social Care (DHSC), the Royal College of General Practitioners (RCGP) and the British Medical Association (BMA) have jointly concluded that there are numerous reasons as to why it is necessary for GP practices to access patient records, even when the patient is no longer a registered patient of the practice. This policy will outline the process to access and share records at Jenner House Surgery.

## 1.2 Status

The practice aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have in regard to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

## 1.3 Training and support

The practice will provide guidance and support to help those to whom it applies understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

# 2 Scope

---

## 2.1 Who it applies to

This document applies to all employees of the practice. Other individuals performing functions in relation to the practice, such as agency workers, locums and contractors, are encouraged to use it.

## 2.2 Why and how it applies to them

GP practices should make decisions about which organisations access their patient records. They should also consider which organisations in the local health community are providing care to their patients and whether information sharing would improve the delivery of care and is necessary for direct care.<sup>1</sup>

# 3 Definition of terms

---

## 3.1 Department of Health and Social Care

---

<sup>1</sup> [Principles for sharing and accessing local shared electronic patient records for direct patient care](#)

The Department of Health and Social Care (DHSC) supports ministers in leading the nation's health and social care to help people live more independent, healthier lives for longer.<sup>2</sup>

### **3.2 Royal College of General Practitioners**

The Royal College of General Practitioners (RCGP) is the professional membership body for GPs in the UK with the purpose of encouraging, fostering and maintaining the highest possible standards in general medical practice.<sup>3</sup>

### **3.3 British Medical Association**

The British Medical Association (BMA) is the trade union and professional body for doctors in the UK.<sup>4</sup>

### **3.4 General Data Protection Regulation**

The GDPR replaced the Data Protection Directive 95/46/EC and has been designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way in which organisations across the region approach data privacy. The GDPR became applicable as law in the UK on 25<sup>th</sup> May 2018.

### **3.5 Explicit consent**

Explicit consent is required for purposes other than the provision of direct care. To conform to the GDPR, consent must be freely given, specific, informed and an unambiguous indication of the data subject's agreement.<sup>5</sup>

### **3.6 Confidentiality<sup>6</sup>**

All identifiable patient information, whether written, computerised, visually or audio recorded, or simply held in the memory of health professionals is subject to the duty of confidentiality. This includes:

- Any clinical information about an individual's diagnosis or treatment
- A picture, photograph, video, audiotape or other image of the patient
- Anything else that, directly or indirectly, might lead to identifying the patient

### **3.7 Information sharing**

The disclosure of personal information from one or more organisations to a third-party organisation or organisations, or information shared internally within an organisation.<sup>7</sup>

---

<sup>2</sup> [DHSC](#)

<sup>3</sup> [RCGP](#)

<sup>4</sup> [BMA](#)

<sup>5</sup> [BMA GPs as data controllers under the GDPR](#)

<sup>6</sup> [BMA Confidentiality](#)

<sup>7</sup> [NHS\(E\) Information Sharing Policy](#)

## 4 Policy

---

### 4.1 Sharing agreements

It is recommended by the BMA that formal sharing agreements are introduced between the practices that will be involved in the sharing process. Jenner House Surgery will use an Information Sharing Agreement, which takes into consideration the General Data Protection Regulation (GDPR) and the [NHS\(E\) Information Sharing Policy](#), ensuring that any information shared is protected and used only for the specified purpose(s).

Furthermore, to maintain GDPR compliance, Jenner House Surgery will ensure that data is processed in accordance with Article 5 of the GDPR and will be able to demonstrate compliance with the regulation (see the GDPR policy for detailed information). Data processors at Jenner House Surgery will ensure that the processing of personal data is lawful and at least one of the following applies:

- The data subject has given consent to the processing of his/her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or another natural person

The Practice Data Protection Officer will support the Practice in the administration of all Information Sharing Agreements.

### 4.2 Legitimate relationships

It is considered appropriate and acceptable for a clinician at Jenner House Surgery to view entries within an individual's healthcare record for the purpose of providing direct care (unless the patient objects), even if the patient is not registered at Jenner House Surgery.

At Jenner House Surgery, clinicians will only view information that is pertinent to the presenting condition of the patient. However, if the patient has given their consent, the clinician can view the patient's full healthcare record.

### 4.3 Access controls

Effective access controls must be in place to prevent unwarranted access to the patient record, unless there is a justified reason and audit is one way of ensuring access controls are effectual. At Jenner House Surgery, it is the responsibility of the Practice Manager to regularly audit access to medical records, and it is considered best practice to ensure that system alerts are in place, which will advise the Practice Manager when a patient's record is accessed by an external organisation.

### 4.4 Privacy

Jenner House Surgery has a duty to advise patients of the purpose of personal data and the methods by which patient personal data will be processed. The practice privacy notice explains what information is collected, how that information may be used and with whom the practice will share that information.

## 4.5 Consent

Consent is appropriate if data processors are in a position to “offer people real choice and control over how their data is used”.<sup>8</sup> The GDPR states that consent must be unambiguous and requires a positive action to “opt in”, and it must be freely given. Data subjects must be made aware that they have the right to withdraw consent at any time. In addition, consent must be clearly identifiable and separate from other comments entered into the healthcare record.

## 4.6 Restrictions

Patients should have the option to restrict what information is shared and must be able to request that certain entries within their healthcare records are marked as ‘sensitive’ and that they are not shared with, or visible to, external organisations or other practices which they may visit for the purpose of direct care. The following key points should be explained to patients:<sup>1</sup>

- Patients can decide not to share their records with any organisation(s)
- Patients can determine which organisations can access their records

Furthermore, the patient must provide explicit consent for a practice other than their registered practice to access their healthcare record.

## 4.7 System specifics

At Jenner House Surgery EMIS Web / Vision is used and there is a requirement to have a local sharing agreement, as referenced at paragraph 3.1, with the following organisations for the purpose of direct care:

### Care Record

Farnborough Locality Care Records  
GP Viewer via MIG  
Phyllis Tuckwel Hospice Care  
SMS Enuresis Service

### Reporting (number data only)

CCG LSC Search/Reports  
QSurveillance Upload

### Data distribution (number data only)

GPES

### Cross Organisational Tasks

Farnborough Locality  
SMS Enuresis Service

---

<sup>8</sup> [ICO Consent](#)

## **Appointments**

SMS Enuresis Service

Farnborough Locality

NHUC Remote Consultation Agreement

## **5 Summary**

---

When there is a requirement to share information for the purpose of providing direct care, it is crucial that the data subject is fully aware of how their information may be shared and who it will be accessed by. Where applicable, information-sharing agreements must be in place and adhered to in order to prevent data breaches.