# Statement of Data Protection Roles and Responsibilities

**Purpose**

This statement sets out the roles and responsibilities of the NHS Business Services Authority (NHSBSA) under Data Protection Legislation as it relates to electronic Repeat Dispensing (eRD) Assurance during the coronavirus emergency.

The NHSBSA will not enter into individual agreements for data protection with Clinical Commissioning Groups (CCGs) and GP practices for this service. This statement coupled with the use of the service gives effect to the data processing relationship between the parties.

This statement meets the requirements of Data Protection Legislation and sets out the following:

* roles of the NHSBSA, NHS England and NHS Improvement, CCGs and GP Practices
* the legal basis for processing
* the subject matter processed
* the duration of the processing
* the type and categories of personal data held and processed
* the responsibilities for Data Subject Rights Requests
* the process for handling breaches
* the process for attributing liabilities

Please note the terms used in this statement are defined in the definitions section at the end of this document.

# 

# Roles

The parties have the following roles, as defined by Data Protection Legislation: -

|  |  |
| --- | --- |
| **Party** | **Role** |
| GP practices | Controller |
| CCGs | Controller |
| NHSBSA | Processor |
| NHS England | Service commissioner |

**Responsibilities**

The parties have the responsibilities detailed in the table below to comply with the GDPR transparency requirement: -

| **Responsibility** | **Details** |
| --- | --- |
| Determine the legal basis of processing (GDPR Article 6) | The NHSBSA understands that the GP practices have the following legal basis:  GDPR Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;;  GDPR Article 9h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;  (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;  Patient Data is being processed in response to the Coronavirus emergency based on a notice issued by the Secretary of State under Regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002  The specific purpose authorised by that notice is *“delivering services to patients, the health services and the public about and in connection with Covid-19, including the provision of information,”* |
| Document the subject matter of the Processing (GDPR Article 30 (b)) | NHSBSA will identify patients who would benefit from electronic repeat dispensing and share this information with the GP practice through their processor the CCG.  The CCG will work with the GP practice to contact the relevant patients to seek their consent to use electronic repeat dispensing. This will involve the CCG sharing the data with the GP practice and encouraging them to clinically review the patients identified to determine if they are suitable for eRD. |
| Document the duration of the Processing (GDPR Article 30 (f)) | NHSBSA and CCG will hold this information until the Coronavirus purpose it is processed for expires, current 30 September 2020.  The GP Practices will determine their own duration and retention in line with their own policies and procedures. |
| Document the nature and purpose of the Processing (GDPR Article 30 (b)) | Identify and contact patients who would benefit from electronic repeat dispensing. This will reduce the patient risk of being exposed to Coronavirus, increase GP practice and pharmacy capacity for seeing other patients and help stabilise demand on supply chain. |
| Document the type of Personal Data (GDPR Article 30 (c)) | * physical or mental health details |
| Document the categories of Data Subjects (GDPR Article 30 (c)) | * NHS patients |
| Responding to Data Subject Rights Requests:  Right of Access (GDPR Article 15)  Right to Rectification (GDPR Article 16)  Right to Erasure (GDPR Article 17) | The GP practice and CCG will action these rights for the requests it receives and the personal data it holds. |
| Providing Privacy Notices to Data Subjects (GDPR Articles 13 - 14) | NHSBSA working with NHS England and NHS Improvement will make CCGs and GP practices aware of the arrangements for this service on the relevant websites and Service portal.  The CCG will make their staff and GP practices aware of the processing they undertake.  GP practices will make their patients aware of the processing they undertake when seeking patient consent. |
| Handling Personal Data Breaches (GDPR Articles 33 - 34) | If the NHSBSA becomes aware that a breach it will advise the affected Controllers.  The Controller will handle personal data breaches relating to the relevant personal data they hold through their normal processes |
| Data Subjects right to compensation and liability (GDPR Article 82) | The CCG and GP practice will be liable for any compensation claims unless the cause is a result of the acts or omissions of the NHSBSA or the CCG. |
| Contact point for Data Subjects (GDPR Article 38) | The Data Protection Officer of the GP practice and CCG |

**Specific Processor Responsibilities**

The Processor shall:

1,Ensure that it has in place appropriate technical and organisational measures to ensure the security of the Personal Data (and to guard against unauthorised or unlawful Processing of the Personal Data and against accidental loss or destruction of, or damage to, the Personal Data), as required under Article 5 (1) f) the ‘integrity and confidentiality’ Principle; and reasonably require to satisfy itself that the Processor is complying with its obligations under Data Protection Legislation;

2 Provide the Controller with such information as the Controller may reasonable request such as the information detailed in Article 28 of GDPR.

3 Not transfer Personal Data outside of the UK and/or the European Economic Area;

4 Only process Personal Data in accordance with, and for the purposes set out in, written instructions received from the Controller from time to time.

5 Notify the Controller promptly and without undue delay, and in any event within 24 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach;

6.Promptly notify the Controller of any instruction received that it believed breaches any data protection law ;

7.Co-operate with the Controller in informing Data Subjects of any Personal Data breach;

8.Ensure it does not knowingly or negligently do or omit to do anything which places the Controller in breach of the Controller’s obligations under Data Protection Legislation;

9.Obtain the Controller’s approval of any sub-contractor and ensure that they are subject to the same contractual obligations as the Processor in this agreement;

10.Permit the Controller at any time and from time to time upon seven days' written notice to have escorted access to the appropriate part of the Processors premises, systems, equipment, and other materials and facilities to enable the Controller to inspect the same for the purposes of monitoring compliance with this Memorandum of Understanding and the Data Protection Act Legislation to the extent that such premises, equipment and other materials and facilities are used for or relevant to the Services. Such inspection shall not relieve the Processor of any of its obligations under this agreement.

11.Where the Processor receives an Data Subject Rights Request (as defined in Articles 15 to 22 of GDPR) from a Data Subject in relation to information which it is holding on behalf of the Controller, it shall (and shall procure that its sub-contractors shall:

* + transfer the Request to the Controller as soon as practicable after receipt and in any event within two (2) Working Days of receiving the Information Rights Request;
  + provide the Controller with a copy of all information in its possession or power in the form that the Controller requires within ten (10) Working Days (or such other period as may be agreed) of the Controller requesting that information; and
  + provide all necessary assistance as reasonably requested to enable the Controller to respond to the Data Subject Rights Request within the time for compliance set out in GDPR.

12.The Controller hereby permits the Processor to store Personal Data relating to (the Personal Data being Processed) on a third party supplier’s system and the Controller permits the Processor’s third party supplier to act as the Processor on its behalf.

13.The provisions of this section shall apply during this agreement and for as long as the Data Protection Legislation requires after its expiry or termination.

**Definitions**

|  |  |
| --- | --- |
| “Controller” | has the meaning given in Data Protection Legislation and "Joint Controllers" has the meaning given in Article 26 GDPR; |
| "Data Protection Legislation" | the Data Protection Act 2018 (DPA), the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to Processing of Personal Data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner; |
| “Data Subject” | has the meaning given in Data Protection Legislation; |
| “Data Subject Rights Request” | a request made by a Data Subject in accordance with rights granted pursuant to Data Protection Legislation to access his or her Personal Data as set out in Articles 15 to 22 of GDPR; |
| “European Law” | European Union or European Member State law (as referred to in the GDPR) or such other law as may be designated in its place when England (whether with Scotland, Wales and/or North Ireland or not), leaves the European Union; |
| "GDPR" | the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council); |
| "Personal Data" | has the meaning given in Data Protection Legislation; |
| “Process” | has the meaning given in Data Protection Legislation and “Processed” and “Processing” shall be construed accordingly; |