[Pharmacy/Contractor Name] Data Protection Impact Assessment (DPIA)

This DPIA template is based on the Information Commissioner’s Office (ICO) template of how you can record your DPIA process and outcome. It follows the process set out in the ICO DPIA guidance, and the [Criteria for an acceptable DPIA](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711) set out in European guidelines on DPIAs.

Also use this template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan. You may further amend or add onto template answers provided and should then add this to your GDPR Booklet.

**KEY:** blue text added by PSNC; red to be completed by you

# Step 1: Identify the need for a DPIA

|  |
| --- |
| Explain broadly what the project aims to achieve, what the anticipated benefits to the pharmacy, patients and others will be and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.  The need is identified based on:   1. The community pharmacy/contractor processes data concerning health, a special category of personal data; 2. The GDPR requires a DPIA to be completed if you process special category data on a large-scale; 3. Guidance indicates that hospitals process data on a large-scale and a single healthcare professional such as a medical doctor does not; 4. Processing of data concerning health in an NHS pharmacy has been introduced primarily through legislation – the NHS (Pharmaceutical and Local Pharmaceutical Services) Regulations 2013, as amended; 5. Government or quasi Government bodies and PSNC are involved in negotiations and discussions regarding legislation and pharmacy practice and assessing relevant risks when the legislation is introduced;   Community pharmacy processing of data concerning health involves some risk of personal data breaches. |

|  |
| --- |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? Will you be collecting new information about individuals? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?   1. Template C in the completed Community Pharmacy GDPR Workbook set out the processing undertaken by the community pharmacy/contractor, how data is collected, used and stored and when data is deleted; as well as the source of the data and with whom the data will be shared. 2. Processes that involve significant risks include: processing NHS prescriptions; supply of dispensed medicines; the Pharmacy Medication Records (PMR) computer system, the use of data capture and recording systems used for commissioned services that are not part of the Essential services under the Community Pharmacy Contractual Framework and managing patient and customer financial data. |

|  |
| --- |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data or biometric data or facial recognition or relate to monitoring a publicly accessible area? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? Will you need to contact individuals in a way which may find intrusive?  PSNC estimates the scale of data processing annually, based on patient prescription nomination data to be:  **How many patient records does a pharmacy have?**  The number of patients nominating a pharmacy could be a proxy for the number of patients’ records held by a pharmacy. Using nomination data has the advantage that it’s (a) nationally available and (b) transparent and (c) doesn’t require contractors to produce a “patient list”. The data at <http://psnc.org.uk/dispensing-supply/eps/patient-nomination-of-a-dispensing-site/nomination-reports/> suggests an average pharmacy has 2,241 nominations based on the total number of nominations (26 million) and the number of community pharmacies (11,600).  EPS prescriptions account for only 60% of prescriptions, so we need to factor in the paper prescriptions which will include the acute conditions treated or one-off prescriptions. If 2,241 patients equate to 60% of the total, **3,735 patients** equate to the (albeit approximate) 100% or total for each pharmacy (on average).  On this basis, on average there will be:  1 pharmacy                        - 3,735 patients  10 pharmacies                   - 37,350 patients  30 pharmacies                   - 112,050 patients  Patients records for those patients for whom you no longer dispense prescriptions would also need to be considered.  While a better estimate of patient records held by a community pharmacy, it may be easier to estimate your scale of processing based on prescription items dispensed.  **What about prescription items?**  We could also look at the total number of prescription items dispensed each year in England, which is approximately 1 billion. If we take the total number of nominations, which is approximately 25 million, this means approximately 40 items per patient per year. This is higher than the data from “Prescriptions dispensed in the Community, Statistics for England 2006-2016”, at <https://digital.nhs.uk/catalogue/PUB30014>, which indicates that each patient in the country has on average 20 items a year, but not all patients have a prescription in any year, so 40 is probably more realistic and it accounts for acute prescriptions.  With approximately 11,600 pharmacies, this means on average 7,000 prescription items monthly or 84,000 annually.  Prescription items gives an indication of the scale of processing of the pharmacy and is easily accessed. It is suggested that you use this as your proxy.  Average number of prescription items dispensed annually by this community pharmacy/contractor:  Additional information in Annex Cs in GDPR Workbook. |

|  |
| --- |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?   1. NHS Community pharmacy processing of data concerning health as part of frontline NHS services for the benefit of patients and the public accessing pharmaceutical services. 2. The community pharmacy is subject to statutory, practice and professional clinical governance requirements. 3. The/each community pharmacy has an Information Governance (IG) lead and the contractor may have a Senior Information Risk Owner (who may be the IG lead in smaller organisations). 4. Staff complete training as required for their roles in accordance with NHS terms of service. 5. Pharmacists and Pharmacy Technicians are subject to a standard of practice and are subject to regulation by the General Pharmaceutical Council. 6. Various procedures to ensure patients consent to aspects of practice, including EPS nominations, choice of community pharmacy and NHS Summary Care Record use. 7. Community pharmacy contractors must meet specified standards against the mandatory annual self-assessment of information governance. 8. The/each community pharmacy/contractor has completed the GDPR Workbook. 9. The community pharmacy is assisted in technical and organisational security and data protection by its Patient Medication Record (PMR) system supplier. |

|  |
| --- |
| **Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?  Provision of Pharmaceutical services for the NHS as independent primary care contractors. |

# Step 3: Consultation process

|  |
| --- |
| **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?  Generally, the processes are dictated by the NHS and requirements are statutory. The government consults as part of the legislative process. As stated, aspects of the provision are subject to (activity) consent or there is consent, explicit or implied, or statutory or overriding public interest provisions to disclose confidential data. |

# Step 4: Assess necessity and proportionality

|  |
| --- |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?   1. Lawful basis for processing health data is set out in Template C in the GDPR Workbook and is generally ‘performance of a duty in the public interest’. 2. The processing achieves the purpose and generally must be processed according to NHS practices and procedures and guidance. 3. Data quality is ensured as part of the NHS system, for example, patient data is usually supplied direct from GP practices as well as checked with patients. 4. Data minimisation is ensured, for example, in data collection and recording systems which provide data to commissioners via third parties, for example a Local Pharmaceutical Committee (LPC), the data is pseudonymised. 5. Patients are provided with information about processes including through practice leaflets and a privacy notice which includes notification of rights. Patients are assisted with prescription queries as a part of professional practice. 6. Checks are made to ensure processors comply with security and data protection standards and are recorded in the GDPR Workbook for the community pharmacy/contractor. One main processor, the PMR supplier, assists the community pharmacy with its security and data protection. 7. There are NHS standards to be met on data security, including for example, the standards for connection to the NHS Spine and use of NHSmail accounts for the transfer of patient data by email within the NHS and the [Data Security and Protection Toolkit](https://www.dsptoolkit.nhs.uk/) (that replaces the IG toolkit). |
| International transfers of data are not carried out by the community pharmacy / are carried out and relevant issues and safeguards are set out below (international transfer of data is not covered in the GDPR Workbook). |

|  |  |  |  |
| --- | --- | --- | --- |
| **Describe the source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risksas necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
| **Processes that involve significant risks include:** | **Remote, possible or probable** | **Minimal, significant or severe** | **Low, medium**  **or high** |
| Processing NHS prescriptions | Possible | Significant | Medium |
| With the supply of dispensed medicines | Probable | Significant | Medium |
| The Patient Medication Records (PMR) computer system | Possible | Significant | Medium |
| The use of data capture and recording systems used for commissioned services that are not part of the Essential services under the Community Pharmacy Contractual Framework | Possible | Minimal | Low |
| Managing patient and customer financial data | Possible | Minimal | Low |
| New surveillance methods such as CCTV may be an unjustified intrusion on a persons’ privacy | Not applicable | Not applicable | Not applicable |

# Step 6: Identify measures to reduce risk

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | | | |
| **Risk** | | **Options to reduce or eliminate risk** | **Effect on risk** | | **Residual risk** | **Measure approved by you** |
|  | |  | **Eliminated, reduced or accepted** | | **Low, medium**  **or high** | **Yes/no** |
| Processing NHS prescriptions | | Standards met; PMR supplier assurances and assurances from other experts | Reduced | | Low | Yes |
| With the supply of dispensed medicines | | e.g. supply of another patient’s repeat slip. SOPs and dispensing checks take place but impossible to eliminate human error | Reduced | | Low | Yes |
| The Patient Medication Records (PMR) computer system | | Standards met; PMR supplier assurances and assurances from other experts | Reduced | | Low | Yes |
|  | | (Additional information in the GDPR Workbook) |  | |  |  |
| **Item** | **Name/position/date** | | | **Notes** | | |
| Measures approved by: | If applicable | | | Integrate actions back into project plan, with date and responsibility for completion | | |
| Residual risks approved by: | If applicable | | | If accepting any residual high risk, consult the ICO before going ahead | | |
| Data Protection Officer (DPO) advice provided: |  | | | DPO should advise on  compliance, step 6 measures and whether processing can proceed  **DPO should provide advice** | | |
| Summary of DPO advice:   * Consider completion and evidence in the GDPR Workbook. * Consider whether culture / implementation of SOPs and other measures takes place – are all the protocols implemented in practice. Can you confirm this? Is there anything additional that needs to be done? | | | |  | | |
| DPO advice accepted or overruled by: |  | | | If overruled, you must explain your reasons | | |
| Comments: If applicable | | | |  | | |
| Consultation responses reviewed by: | If applicable | | | If your decision departs from individuals’ views, you must explain your reasons | | |
| Comments: If applicable | | | |  | | |
| This DPIA will be kept under review by: |  | | | The DPO should also review ongoing compliance with DPIA | | |