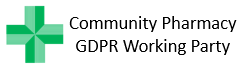
The General Data Protection Regulation and associated legislation

Part 3: Workbook for Community Pharmacy

Version 1: 25th March 2018



**Contents**

[Template A: **D**ecide who is responsible 3](#_Toc509930886)

[Template B: **A**ction Plan 4](#_Toc509930887)

[Template C: **T**hink about and record the personal data you process; 5](#_Toc509930888)

[**A**ssure your lawful basis for processing 5](#_Toc509930889)

[Template D: **P**rocess according to data protection principles 15](#_Toc509930890)

[Template E: **R**eview and check with your processors 16](#_Toc509930891)

[Template F: **O**btain consent if you need to 18](#_Toc509930892)

[Template G: **T**ell people about your processes: the Privacy Notice 19](#_Toc509930893)

[Template H: **E**nsure data security 22](#_Toc509930894)

[Template I: **C**onsider personal data breaches 26](#_Toc509930895)

[Template K: **T**hink about data subject rights 32](#_Toc509930896)

[Template L: **E**nsure privacy by design and default 34](#_Toc509930897)

[Template M: **D**ata protection impact assessment (DPIA) 35](#_Toc509930898)

# Template A: Decide who is responsible

**Pharmacy company/contractor** Click or tap here to enter text.

The pharmacy company/contractor is the data controller and is responsible/accountable for data protection and implementation of the GDPR.

**Senior staff member responsible for GDPR compliance** Click or tap here to enter text.

(add name and job title)

**IG Lead and/or** Click or tap here to enter text.

**Senior Information Risk Owner (SIRO)**

(add name and job title: in smaller organisations the same person may be both; in larger organisations, there may be one SIRO and an IG Lead for each community pharmacy)

**Superintendent pharmacist (if applicable)** Click or tap here to enter text.

(add name)

**Caldicott Guardian** Click or tap here to enter text.

(add name and job title)

**Summary Care Record (SCR) Governance** Click or tap here to enter text.

**Person**

(add name and job title)

**Data Protection Officer (if required)** Click or tap here to enter text.

(add name and contact details)

The DPO may, or may not, be a member of staff. The DPO has responsibilities set out in the GDPR – guidance may be found in the Information Governance Alliance’s guidance ‘*The GDPR Data Protection Officer’* at <https://www.digital.nhs.uk/article/1414/General-Data-Protection-Regulation-guidance>. The DPO should advise you on your obligations under the GDPR and should have expert knowledge of data protection law. You may want to appoint a DPO even if you are not required to do so.

# Template B: Action Plan

**Plan for implementation Date achieved**

Decide who is responsible (DPO not completed) Click or tap here to enter text.

Action plan Click or tap here to enter text.

Think about and record the personal data you process Click or tap here to enter text.

Assure your lawful basis for processing Click or tap here to enter text.

Process according to data protection principles (Policies) Click or tap here to enter text.

Review and check with your processors Click or tap here to enter text.

Obtaining consent if you need to Click or tap here to enter text.

Tell people about your processes: the Privacy Notice Click or tap here to enter text.

Ensure data security Click or tap here to enter text.

Consider personal data breaches Click or tap here to enter text.

Think about data subject rights Click or tap here to enter text.

Ensure privacy by design and default Click or tap here to enter text.

Data protection impact assessment Click or tap here to enter text.

DPO appointed, if required Click or tap here to enter text.

Relevant ICO number Click or tap here to enter text.

Paid current annual fee to the ICO Click or tap here to enter text.

**The senior staff member responsible for GDPR compliance,** **IG and data security (e.g. SIRO/IG Lead as applicable) has signed off the policies and procedures in this workbook and related policies and procedures**

*(Name, date and sign)*Click or tap here to enter text.

Annual review date Click or tap here to enter text.

# Template C: Think about and record the personal data you process;

# Assure your lawful basis for processing

**Activity: Receipt, dispensing and submission of NHS paper and electronic prescriptions, including, for example, repeatable prescriptions and related tokens and manual unstructured files of prescriptions.**

|  |  |
| --- | --- |
| **Pharmacy status** | Data Controller |
| **Data subjects and personal data** | Personal data such as patient name, address, contact details, medicines and relevant health data. |
| **Purpose** | Care of the patient, pharmacy payment and NHS management. |
| **Lawful basis for processing personal data** | Article 6(1)(e) of the GDPR. Necessary for the performance of a task in the public interest. |
| **Special category of personal data** | Yes, data concerning health (this could include information on a disability). The data may also be another special category of personal data. |
| **Basis for processing special category of data** | Article 9(2)(h) of the GDPR (including the Data Protection Act). ‘The provision of health care or treatment’ or ‘the management of health care systems or services or social care systems or services’ or ‘necessary for reasons of public health in the area of public health’. |
| **How is data collected?** | The patient, or patient’s representative, a prescription, healthcare professional, or the SCR record, as appropriate. |
| **How is data stored?** | Primarily the PMR system, but also e-mail or equivalent (if so, consider security), CD or Specials registers, as relevant and necessary. Manual unstructured files stored in the pharmacy. |
| **How long is data stored?** | According to NHS guidance – the *Recommendations for the Retention of Pharmacy Records - prepared by the East of England NHS Senior Pharmacy Managers 2016* in this case the life of the patient plus 10 years. |
| **To whom do you provide the data (recipients)? (including processors)** | GP practices, NHS Business Services Authority and others in the NHS (e.g. hospitals on admission), and only relevant information to those external to the NHS who negotiate and check our payments; relevant information to NHS organisations and others such as the GPhC for compliance and enforcement purposes. Processors: Click or tap here to enter text. |
| **Date confirmed that this applies to your pharmacy** | Click or tap here to enter text. |

Template C continued

**Activity: Advanced services such as Medicines Use Reviews (MURs), the New Medicine Service (NMS), the NHS Urgent Medicine Supply Advanced Service (NUMAS), Appliance Use Reviews (AUR), Stoma Appliance Customisation (SAC) and the Flu Vaccination Service. Add or remove services as appropriate.**

|  |  |
| --- | --- |
| **Pharmacy status** | Data Controller |
| **Data subjects and personal data** | Personal data such as patient name, address, contact details, medicines and relevant health data. |
| **Purpose** | Care of the patient, pharmacy payment and NHS management. |
| **Lawful basis for processing personal data** | Article 6(1)(e) of the GDPR.  Necessary for the performance of a task in the public interest. |
| **Special category of personal data** | Yes, data concerning health (this could include information on a disability). The data may also be another special category of personal data. |
| **Basis for processing special category of data** | Article 9(2)(h) of the GDPR (including the Data Protection Act).  ‘The provision of health care or treatment’ or ‘the management of health care systems or services or social care systems or services’ or ‘necessary for reasons of public health in the area of public health’. |
| **How is data collected?** | The patient, or the patient’s representative, a prescription, another healthcare professional, the SCR record, and Advanced Service form, as appropriate. |
| **How is data stored?** | Hard copy or electronic (PMR system) records, and hard copy consent forms as appropriate. |
| **How long is data stored?** | Click or tap here to enter text. |
| **To whom do you provide the data (recipients)? (including processors)** | GP practices, NHS Business Services Authority and others in the NHS (e.g. hospitals on admission), and only relevant information to those external to the NHS who negotiate and check our payments; relevant information to NHS organisations and others such as the GPhC for compliance and enforcement purposes. Processors: Click or tap here to enter text. |
| **Date confirmed that this applies to your pharmacy** | Click or tap here to enter text. |

Template C continued

**Activity: Enhanced and other local commissioned services – list as relevant.**

|  |  |
| --- | --- |
| **Pharmacy status** | Data Controller |
| **Data subjects and personal data** | Personal data such as patient name, address, contact details, medicines and relevant health data. |
| **Purpose** | Care of the patient, pharmacy payment and NHS management. |
| **Lawful basis for processing personal data** | Article 6(1)(e) of the GDPR.  Necessary for the performance of a task in the public interest. |
| **Special category of personal data** | Yes, data concerning health (this could include information on a disability). The data may also be another special category of personal data. |
| **Basis for processing special category of data** | Article 9(2)(h) of the GDPR (including the Data Protection Act).  ‘The provision of health care or treatment’ or ‘the management of health care systems or services or social care systems or services’ or ‘necessary for reasons of public health in the area of public health’. |
| **How is data collected?** | Specific to the local service; details included in the service specification. |
| **How is data stored?** | Specific to the local service; details included in the service specification. |
| **How long is data stored?** | Click or tap here to enter text. |
| **To whom do you provide the data (recipients)? (including processors)** | Click or tap here to enter text. |
| **Date confirmed that this applies to your pharmacy** | Click or tap here to enter text. |

Template C continued

**Activity: Additional records associated with dispensing medicines, for example, repeat dispensing, public health (promotion of healthy lifestyles), signposting and support for selfcare records; and other pharmacy records, for example, patient safety log, delivery services (a non-NHS service) and pharmacy audits.**

|  |  |
| --- | --- |
| **Pharmacy status** | Data Controller |
| **Data subjects and personal data** | Personal data such as patient name, address, contact details, medicines and relevant health data. |
| **Purpose** | Care of the patient, pharmacy payment and NHS management. |
| **Lawful basis for processing personal data** | Article 6(1)(e) of the GDPR.  Necessary for the performance of a task in the public interest. |
| **Special category of personal data** | Yes, data concerning health (this could include information on a disability). The data may also be another special category of personal data. |
| **Basis for processing special category of data** | Article 9(2)(h) of the GDPR (including the Data Protection Act ).  ‘The provision of health care or treatment’ or ‘the management of health care systems or services or social care systems or services’ or ‘necessary for reasons of public health in the area of public health’. |
| **How is data collected?** | Click or tap here to enter text. |
| **How is data stored?** | Primarily the PMR system, but also e-mail or equivalent, CD or Specials registers, as relevant and necessary. |
| **How long is data stored?** | Click or tap here to enter text. |
| **To whom do you provide the data (recipients)? (including processors)** | As appropriate: GP practices, NHS Business Services Authority and others in the NHS (e.g. hospitals on admission), only relevant information to Local authorities, Clinical Commissioning Groups, to those external to the NHS who negotiate and check our payments; and to NHS organisations and others such as the GPhC for compliance and enforcement purposes. |
| **Date confirmed that this applies to your pharmacy** | Click or tap here to enter text. |

Template C continued

**Activity: Check RX payment data – if applicable**

|  |  |
| --- | --- |
| **Pharmacy status** | Data Controller |
| **Data subjects and personal data** | Personal data such as patient name, address, contact details, medicines and relevant health data. |
| **Purpose** | Pharmacy payment. |
| **Lawful basis for processing personal data** | Article 6(1)(e) of the GDPR.  Necessary for the performance of a task in the public interest. |
| **Special category of personal data** | Yes, data concerning health (this could include information on a disability). The data may also be another special category of personal data. |
| **Basis for processing special category of data** | Article 9(2)(h) of the GDPR (including the Data Protection Act).  ‘The management of health care systems or services or social care systems or services’. |
| **How is data collected?** | From patients and processed by NHSBSA and in pseudonymised form by the Pharmaceutical Services Negotiating Committee. |
| **How is data stored?** | Primarily the PMR system and check Rx systems. |
| **How long is data stored?** | Click or tap here to enter text. |
| **To whom do you provide the data (recipients)? (including processors)** | No-one. |
| **Date confirmed that this applies to your pharmacy** | Click or tap here to enter text. |

Template C continued

**Activity: Private Prescriptions**

|  |  |
| --- | --- |
| **Pharmacy status** | Data Controller |
| **Data subjects and personal data** | Personal data such as patient name, address, contact details, medicines and relevant health data. |
| **Purpose** | Care of the patient. |
| **Lawful basis for processing personal data** | Article 6(1)(e) of the GDPR.  Necessary for the performance of a task in the public interest. |
| **Special category of personal data** | Yes, data concerning health (this could include information on a disability). The data may also be another special category of personal data. |
| **Basis for processing special category of data** | Article 9(2)(h) of the GDPR (including the Data Protection Act).  ‘The provision of health care or treatment’ or ‘the management of health care systems or services or social care systems or services’ or ‘necessary for reasons of public health in the area of public health’. |
| **How is data collected?** | The patient, or the patient’s representative, a prescription, another healthcare professional, or the SCR record, as appropriate. |
| **How is data stored?** | Primarily the PMR system, but also e-mail or equivalent (if so, consider security), POM, CD or Specials registers, as relevant and necessary. Also, hard copy prescription. |
| **How long is data stored?** | Click or tap here to enter text. |
| **To whom do you provide the data (recipients)? (including processors)** | As appropriate: NHS Business Services Authority (only controlled drug prescriptions for schedule 2 and 3 drugs for information, not payment) and relevant information to others in the NHS (e.g. as appropriate, GP practice, hospital on admission); relevant information to others such as the GPhC for compliance and enforcement purposes. |
| **Date confirmed that this applies to your pharmacy** | Click or tap here to enter text. |

Template C continued

**Activity: Other non-NHS care services**

|  |  |
| --- | --- |
| **Pharmacy status** | Data Controller |
| **Data subjects and personal data** | Personal data such as patient name, address, contact details, medicines and relevant health data. |
| **Purpose** | Care of the patient. |
| **Lawful basis for processing personal data** | Article 6(1)(e) of the GDPR.  Necessary for the performance of a task in the public interest. |
| **Special category of personal data** | Yes, data concerning health (this could include information on a disability). The data may also be another special category of personal data. |
| **Basis for processing special category of data** | Article 9(2)(h) of the GDPR (including the Data Protection Act).  ‘The provision of health care or treatment’ or ‘the management of health care systems or services or social care systems or services’ or ‘necessary for reasons of public health in the area of public health’. |
| **How is data collected?** | Click or tap here to enter text. |
| **How is data stored?** | Click or tap here to enter text. |
| **How long is data stored?** | Click or tap here to enter text. |
| **To whom do you provide the data (recipients)? (including processors)** | Click or tap here to enter text.  Relevant information to other organisations such as the GPhC for compliance and enforcement purposes. |
| **Date confirmed that this applies to your pharmacy** | Click or tap here to enter text. |

Template C continued

**Activity: Employment records**

|  |  |
| --- | --- |
| **Pharmacy status** | Data Controller |
| **Data subjects and personal data** | Personal data such as employee name, address, contact details, staff appraisals, contracts. |
| **Purpose** | Employment purposes – and tax and National Insurance purposes. |
| **Lawful basis for processing personal data** | Article 6(1)(e) of the GDPR.  Necessary for the performance of a task in the public interest. |
| **Special category of personal data** | Yes, health data and DBS checks, as appropriate |
| **Basis for processing special category of data** | Article 9(2)(b) ‘is necessary for the purposes of carrying out the obligations and exercising the specific rights … in the field of employment …social law protection in so far as it is authorised in the Union or Member State law…’ for health data  [Article 10 and Section 9 and 10 of the Data Protection Act 2018 for DBS checks] |
| **How is data collected?** | From employees and referees. |
| **How is data stored?** | Click or tap here to enter text. |
| **How long is data stored?** | Click or tap here to enter text.  (e.g. term of employment and 7 years) |
| **To whom do you provide the data (recipients)?**  **(including processors)** | Click or tap here to enter text.  (company which is a processor for payroll purposes only) |
| **Date confirmed that this applies to your pharmacy** | Click or tap here to enter text. |

Template C continued

**Activity:** Click or tap here to enter text.

|  |  |
| --- | --- |
| **Purpose** | Click or tap here to enter text. |
| **Lawful basis for processing personal data** | Click or tap here to enter text. |
| **Special category of personal data** | Click or tap here to enter text. |
| **Basis for processing special category of data** | Click or tap here to enter text. |
| **How is data collected?** | Click or tap here to enter text. |
| **How is data stored?** | Click or tap here to enter text. |
| **How long is data stored?** | Click or tap here to enter text. |
| **To whom do you provide the data (recipients)?** | Click or tap here to enter text. |
| **Date confirmed that this applies to your pharmacy** | Click or tap here to enter text. |

Template C continued

Retention of records

The following may be helpful in considering retention periods:

A copy of the NHS guidance – the *Recommendations for the Retention of Pharmacy Records – prepared by the East of England NHS Senior Pharmacy Managers 2016*

<https://www.sps.nhs.uk/articles/retention-of-pharmacy-records/>

*Records Management Code of Practice for Health and Social Care 2016* <https://digital.nhs.uk/records-management-code-of-practice-for-health-and-social-care-2016>

Records may be kept for longer periods than the legal minimum retention period. The retentions periods used should be retained as part of the workbook included in each Template C.

Common Law Duty of confidence (confidentiality)

The common law duty of confidence (confidentiality) continues to apply to healthcare practice and the courts have recognised three broad circumstances under which confidential information may be disclosed:

• consent – whether express or implied (implied consent means that the subject knows or would reasonably expect the proposed use or disclosure and has not objected)

• authorised or required by law, for example under statute, common law (including duty of care) or legal proceedings.

• Overriding public interest, for example where a patient is contagious or the public is at risk, such that there is a public interest in disclosure that overrides the public interest in maintaining confidentiality.

(This is a partial quote from the Information Governance Alliance (IGS) booklet on Guidance on Lawful Processing.)

Responsibility for Processing Personal data

Under the GDPR, a healthcare professional (such as a pharmacist or a pharmacy technician subject to registration and regulatory oversight e.g. as per the Pharmacy Order 2010), social work professional or a person with a duty of confidentiality under a legal provision, must be responsible for the processing of data concerning health.

# Template D: Process according to data protection principles

To process personal data in accordance with data protection principles you must have suitable policies in place. The policies supporting the [IG Toolkit](https://psnc.org.uk/ds) 2017/18 are listed at the end of this workbook and you may have many of these already. These will be added to or amended by (the templates in) this booklet and the other guidance documents (Part 1 and 2).

Following the data protection principles involves for example:

|  |  |
| --- | --- |
| **Principle** | **Issues to consider** |
| Lawfully | All your processing is lawful – templates C and F  Also, responsibilities, DPO, action plan, ICO fee and sign off – templates A and B |
| Fairly and transparent | A privacy notice is provided, any objections to processing are considered and data breaches dealt with appropriately – see templates G, I, J and K  Also, processors’ contracts are appropriate – see template E |
| Adequate, relevant and limited for the purposes | Personal data available only to those who need to see it for the work they do – privacy by design and default apply and Data Protection Impact Assessments are carried out if required – see templates L and M  Also, processors’ contracts are appropriate – see template E |
| Accurate/up to date | Records are accurate and, if relevant, up to date – see template H (Data Quality) |
| Form in which identification kept for no longer than necessary | Pseudonymisation/redaction of personal details, has been considered, as appropriate – consider privacy by design and default – see template L |
| Security | There is appropriate physical, electronic and human security – see template H |
| Integrity | Data is backed up so that it is protected against accidental loss or damage – see template H |

# Template E: Review and check with your processors

Identify your processors and ensure that your **contracts** with them are GDPR compliant.

Your existing contractual terms may already comply, your first step should be to check this or seek clarification from your processors.

Your processors may include your PMR system supplier, PMR intermediate aggregator company, any person providing data capture and reporting systems (such as PharmOutcomes), any external body that undertakes your payroll for you and anybody who transfers your prescription bundles to the NHS Business Services Authority (NHS BSA).

List your processors and confirm any assurances sought and received.

|  |  |  |  |
| --- | --- | --- | --- |
| **Processor, product and service** | **Date assurances requested** | **Date confirmation received from processor** | **Date contract ends** |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |

You should be able to rely on your processors to provide you with the necessary guarantees listed on the next page.

You may only use those processors providing sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the GDPR and ensure the security of the data and that you can meet any data subject right.

Your processors should be cross-checked with your information asset register which lists your pharmacy hardware and software.

You are likely to be a processor for other data controllers, in which case you may have to provide information and assurances to them.

The ICO indicates that contracts with processors:

Must set out:

* the subject matter and duration of the processing;
* the nature and purpose of the processing;
* the type of personal data and categories of data subject; and
* the obligations and rights of the controller.

Must also include as a minimum the following terms requiring the processor to:

* only act on the written instructions of the controller;
* ensure that people processing the data are subject to a duty of confidence;
* take appropriate measures to ensure the security of processing;
* only engage sub-processors with the prior consent of the controller and under a written contract;
* assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
* assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
* delete or return all personal data to the controller as requested at the end of the contract; and
* submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

**More information is available from the ICO, but we would expect your processors to ensure that their contracts with you are GDPR compliant.**

# Template F: Obtain consent if you need to

**Note:** Pharmacies have a lawful basis for processing personal data because of the performance of a task carried out in the public interest (stage 1) and for the provision of health or social care or treatment or the management of health or social care systems (stage 2). For other activities, you may need to obtain consent for the processing of personal data.

**Consent**

If you process personal data lawfully by consent, from 25th May 2018, the consent must be GDPR compliant **and** recorded.

‘Consent’ of the data subject under the GDPR means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent gained by pre-ticked consent boxes is not valid consent under the GDPR.

If you process a special category of personal data (such as data concerning health) by consent, you must have the **explicit consent** of the patient/data subject.

**Explicit consent** is intended to be more specific than ‘consent’, and must be confirmed in words, rather than by any other positive action i.e. the person giving consent must signal agreement to an explicit statement in words such as ‘I consent to emails about your products and special offers’ (followed by a tick box to be completed, or not, as the case may be).

If you collect personal data for marketing purposes, you should read the ICO’s guidance on [consent](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

|  |  |  |
| --- | --- | --- |
| **Filing system / activity** | **GDPR compliant consent/explicit consent obtained** | **GDPR compliant consent/explicit consent recorded** |
| The pharmacy has a loyalty card | Consent obtained on  Click or tap here to enter text.  *(Date)* | Consent recorded in  Click or tap here to enter text.  *(Name filing system/computer)* |
|  |  |  |
|  |  |  |

# Template G: Tell people about your processes: the Privacy Notice

When you collect personal data from a data subject you must provide the data subject with relevant information; the Privacy Notice. This should be available on the pharmacy premises, for example, in a poster or the practice leaflet, and, if appropriate, on the pharmacy website; and you should draw the attention of new customers to the Privacy Notice. Draft shorter and longer forms of notice are as follows.

*(name and address)* **PHARMACY PRIVACY NOTICE**

We process your personal data, which includes your name, contact details, prescription medicines and data from other pharmacy and health care services we provide to you (including, for example, pharmacy medicines, medicine use reviews, flu vaccinations and stop smoking services) for the purposes of:

**Your care** – providing pharmacy services and care to you and, as appropriate, sharing your information with your GP and others in the wider NHS;

**Our payments** – sharing your information with the NHS Business Services Authority, others in the wider NHS, and sometimes Local Authorities, and only limited information to those external to the NHS who negotiate and check the accuracy of our payments; and,

**Management** – sharing only limited information with the NHS Business Services Authority and others in the wider NHS, and sometimes Local Authorities; as well as those external to the NHS who ensure we maintain appropriate professional and service standards and that your declarations and ours are accurate.

We hold your information for as long as advised by the NHS. You have a right to a copy of the information we hold about you, generally without charge. You may seek to correct any inaccurate information.

We process your personal data in the performance of a task in the public interest, for the provision of healthcare and treatment and the management of healthcare systems. A pharmacist is responsible for the confidentiality of your information. You may object to us holding your information. You may also lodge a complaint with the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please ask if you want more information. **[You may choose to opt out of the NHS using your data for planning and research purposes – please ask for details.]**

**[Our Data Protection Officer is *(name and contact details)*]**

**Our pharmacists and their staff are members of your local healthcare team.**

**They aim to provide you with the highest quality of healthcare. To do this they need to keep records about you, your health and the care we have provided or plan to provide to you.**

**We know that you value your privacy and the security of personal information held about you.**

**Information recorded**

As part of providing a professional, safe and efficient service, there is certain information that we record. This includes details of drugs and appliances dispensed against NHS prescriptions as well as significant advice given, and referrals made to other health professionals and any other relevant information.

Information recorded may include:

* basic details about you, such as address, date of birth, next of kin;
* records of medicines you have been prescribed by your doctor or another qualified prescriber, and which have been supplied by this pharmacy;
* details of medicines purchased from the pharmacy without a prescription (“over the counter medicines”);
* other details and notes about your health and medical treatment;
* information relevant to your continued care from other people who care for you

and know you well, such as other health professionals and relatives; and

* any other services we provide to you, for example, a flu vaccination.

**Processing Information**

We process your personal data, which includes

information from your prescriptions and any other pharmacy and health care services we provide to you (including medicines use reviews, flu vaccinations, stop smoking services etc.) for the purposes of:

**Your care** – providing pharmacy services and care to you and, as appropriate, sharing your information with your GP and others in the wider NHS;

**Our payments** – sharing your information with the NHS Business Services Authority, others in the wider NHS, and sometimes Local Authorities, and only limited information to those external to the NHS who negotiate and check the accuracy of our payments; and,

**Management** – sharing only limited information with the NHS Business Services Authority and others in the wider NHS, and sometimes Local Authorities; as well as those external to the NHS who ensure we maintain appropriate professional and service standards and that your declarations and ours are accurate.

We hold your information for as long as advised by the NHS.

We process your personal data in the performance of a task in the public interest for the provision of healthcare and treatment. A pharmacist is responsible for the confidentiality of your information.

**[Additional information/ more detail may need to be added]**

**Your Rights**

You have the right to confidentiality under the General Data Protection Regulation and [the Data Protection Act 2018] and the common law duty of confidence.

We also comply with the NHS Code of Practice on Confidential Information and pharmacists have a requirement under their professional standards to keep records about you confidential, secure and accurate.

All of our staff contracts of employment contain a requirement to keep patient information confidential.

**[You may choose to opt out of the NHS using your data for planning and research purposes – please ask for details.]**

**Our guiding principle is that we process your records in strict confidence.**

**Your right to view your health record**

You have the right to ask for a copy of all pharmacy records about you (generally in paper or electronic form).

Generally, there will be no charge for a printed copy of the information we hold about you. We are required to respond to your request within one month.

You will need to give adequate information in order for pharmacy staff to identify you (for example, full name, address and date of birth). You will be required to provide ID, for example a passport, full driving licence or credit/debit card before any information is released to you.

If you think any information we hold on you is inaccurate or incorrect, please let us know.

You may object to us holding your information.

You may lodge a complaint with the Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

**[Our Data Protection Officer is *(name and contact details)*]**

**How we look after and safeguard information about you**





# Template H: Ensure data security

The GDPR requires data controllers to take appropriate technical and organisational measures, and adopt appropriate policies, to ensure personal data is processed securely.

Existing measures should be reviewed recognising that some people do seek unauthorised access to personal data.

The policies listed below that are current and not updated as part of this booklet, will be updated during 2018.

You also need to ensure data quality.

|  |  |  |
| --- | --- | --- |
| **Security issues** | **Measures** | **Date measures confirmed** |
| Physical | The following existing policies should be in place:  Template 6: [[Asset Register](http://www.psnc.org.uk/wp-content/uploads/2013/07/template_6_316__asset_register_version_2.doc)](https://psnc.org.uk/dstemplates) (MS Word) / [Asset Register](https://psnc.org.uk/dstemplates) (MS Excel)  Template 7: [Physical Security Risk Assessment](https://psnc.org.uk/dstemplates)  Click or tap here to enter text. | Click or tap here to enter text. |
| Electronic | The following existing policies should be in place:  Template 8: [Mobile Computing Guidelines](https://psnc.org.uk/dstemplates)  Template 9: [Portable equipment](https://psnc.org.uk/dstemplates) / [Asset control form](https://psnc.org.uk/dstemplates)  Template 10: [Disposal of Portable Assets](https://psnc.org.uk/dstemplates)  You must list and carry out a risk assessment for any of your computer systems that do not have an individual log-in and mitigate the risks associated with these systems.  Your pharmacy system suppliers’ aggregator helps to enable a secure connection and may have signed NHS Digital’s Health and Social Care Network ‘Connection Agreement’ (previously known as the ‘Code of Connection’). EPS prescription data must be sent to NHS Digital’s central ‘Spine’ by pharmacy contractors via the NHS Digital Managed Health and Social Care Network (previously known as N3).  The standards of NHS mail are laid out within your user agreement, and further practical considerations are listed at [PSNC’s NHSmail webpage](http://psnc.org.uk/nhsmail). Learn how to use NHSmail safely, i.e. note that patient data can be communicated securely when both sender and recipient are using an NHSmail account.  Fax machines should only be used to send sensitive data as a very last resort and, when used, staff should consider local [“Safe Haven” procedures.](http://psnc.org.uk/wp-content/uploads/2017/05/Safe-haven-policy-archive-HSCIC-2016-document.doc) Fax numbers should be checked and verified before confidential information is sent to them.  You can monitor systems and logs for unusual activity that might pre-emptively indicate an attack on your system. Your system supplier or IT department may assist with this.  Maintain awareness of cyber risks, e.g. staff should be made aware of the risks from scam, faked or ‘phishing’ (information-seeking) emails, and be wary of clicking on internet links within emails.  Carefully consider the “[Ten steps to help improve data and cyber security within your pharmacy](http://psnc.org.uk/datasteps)” briefing document which includes further information about electronic data security.  Click or tap here to enter text. | Click or tap here to enter text. |
| Human | The following existing policies should be in place:  Template 2: [Staff Confidentiality Agreement](https://psnc.org.uk/dstemplates)  Template 3: [Staff Confidentiality Code](https://psnc.org.uk/dstemplates)  (Staff monitoring of access to personal data is also required)  Template 4: [Data Handling Procedure](https://psnc.org.uk/dstemplates)  Template 13: [Audit Sheet](https://psnc.org.uk/dstemplates)  Template 14: [Staff Signature List](https://psnc.org.uk/dstemplates)/ [Staff Signature List](https://psnc.org.uk/dstemplates) (Separate List)  Template 15: [Access Control and Password Management Procedure](https://psnc.org.uk/dstemplates)   Template 16: [Ensuring Staff Compliance with RA01 Terms Template SOP](https://psnc.org.uk/dstemplates)  Click or tap here to enter text. | Click or tap here to enter text. |

Community pharmacy businesses may need to rely on appropriate experts to provide the relevant technical assurances, for example, their PMR suppliers and PharmOutcomes or others providing technical support and ensure you comply with the technical standards required by the NHS.

You should review your data security policies and practices at least annually, we suggest when you complete the [IG Toolkit](https://psnc.org.uk/ds), to ensure the security of data is maintained. Any personal data breaches may result in a review of policies and a review of the incident management procedures.

Also consider manual unstructured files such as a book recording telephone calls from General Practitioners to ensure such personal data is secure.

*Note: The resources referenced within this Template H, and related guidance may be further updated in the future.*

Template H: Continued

**DATA QUALITY**

There should also be effective data quality controls in place and the policy could be that only authorised members of staff may add to, amend or delete personal data such as a patient’s name or address, or prescription information, from the PMR computer system or any other filing system in the pharmacy.

|  |  |
| --- | --- |
| **Activity** | **Staff names or groups of staff** |
| Adding information | e.g. Dispensary staff |
| Amending information | e.g. Dispensary staff but a pharmacist to approve any amendment to the prescription information recorded and consider whether a correction note should be added rather than any information deleted |
| Deleting information | e.g. Only the IG Lead may delete a patient record |
| Click or tap here to enter text. | Click or tap here to enter text. |
| Click or tap here to enter text. | Click or tap here to enter text. |

# Template I: Consider personal data breaches

**(IG Template 11 updated)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name of Pharmacy  **Pharmacy LogoInformation Security Incident Management Procedures** | | | | |
| Procedures Prepared by:  Click or tap here to enter text. | Procedures Approved by:  Click or tap here to enter text. | Date Next Review Due: | Click or tap here to enter text. |  |
| Date Prepared:  Click or tap here to enter text. | Date Approved:  Click or tap here to enter text. | Date Review Takes Place: | Click or tap here to enter text. |  |

*Information security incidents are any event that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual, the integrity of the system or data put at risk or the availability of the information through the system being put at risk. Incidents may include theft, misuse or loss of equipment containing confidential information or other incidents that could lead to authorised access to data.*

*‘Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

**1. Procedures for dealing with various types of Incident**

All staff should report any suspicious incidents to Click or tap here to enter text. [enter details e.g. the pharmacist in charge or the IG Lead].

Incidents should always be investigated immediately whilst there is still the possibility of collecting as much evidence as possible. Investigations should normally be co-ordinated between at least Click or tap here to enter text. [enter details e.g. the pharmacist in charge or the IG Lead].

The following procedures should be followed for particular personal data breaches:

A) Theft of equipment holding confidential information and unauthorised access to an area with unsecured confidential information:

* Check the asset register to find out which equipment is missing.
* Investigate whether there has been a legitimate reason for removal of the equipment (such as repair or working away from the usual base).
* If the cause is external inform the police and ask them to investigate.
* If the cause is internal, establish the reason for the theft/ unauthorised access.
* Consider whether there is a future threat to system security and the need to take protective action e.g. change passwords.

B) Access to patient records by an authorised user who has no work requirement to access the record:

* Interview the person reporting the incident to establish the cause for concern.
* Establish the facts by;

- Asking the system supplier to conduct an audit on activities by the user concerned.

- Interviewing the user concerned.

* Establish the reason for unauthorised access.
* Take appropriate disciplinary action and action with the patient(s) where appropriate.

C) Inadequate disposal of confidential material (paper, PC hard drive, disks/tapes):

This type of incident is likely to be reported by a member of the public, a patient affected, or a member of staff;

* Investigate how the data came to become inappropriately disposed.
* Take appropriate action to prevent further occurrences (e.g. disciplinary, advice/training, contractual).

D) Procedure for dealing with complaints about patient confidentiality by a member of the public, patient or member of staff:

* Interview the complainant to establish the reason for the complaint. (Note, any complaint by a patient in relation to his NHS services must be investigated and handled in accordance with the Terms of Service.)
* Investigate according to the information given by the complainant and take appropriate action.
* Take appropriate action with the patient(s) as appropriate.
* Categorise and report the incident as described as per ‘recording and reporting’ requirements.

E) Loss of data in transit e.g. when posting MUR forms to the GP surgery or sending prescriptions to NHS Prescription Services.

* Investigate, as far as possible what has gone missing and where.
* Take appropriate action to prevent further occurrences (e.g. was the envelope correctly addressed, is there further safeguards that could be introduced).

**2. Procedures for recording incidents**

A record of all incidents, including near-misses, should be made by completing a copy of the information security incident report form (section 3 below).

Incidents should be classified in the log according to the severity of risk to patients and the pharmacy using the following incident classification system described below. For near-misses, consider the likely impact if the breach had occurred.

You must document any personal data breaches, as above, even if they are not notified to the ICO. The ICO may inspect your records to verify you are keeping such records.

Incident or personal data breach classification:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Insignificant:  (very low risk)  Minimal risk -indiscernible effect on patients or the pharmacy  Not reported to ICO  No patients informed  Recorded as a personal data breach | Minor:  (low risk)  Minor breach, for example data lost but files encrypted, less than 5 patients affected  Not reported to ICO  No patients informed  Recorded as a personal data breach | Moderate:  (Likely to result in a **risk** to the rights and freedoms of patients)  Moderate breach, for example unencrypted clinical records lost, up to 20 patients affected  Reported to ICO  Communication to patients considered  Recorded as a personal data breach | Major:  (Consider whether likely to result in a **high risk** to the rights and freedoms of patients)  Serious breach, for example unencrypted clinical records lost, **up to 1,000 patients** affected or particular sensitivity  Reported to ICO  Communication to patients considered  Recorded as a personal data breach | Critical:  (Likely to result in a **high risk** to the rights and freedoms of patients)  Serious breach in terms of volume of records, for example **over 1,000 patients** affected or particular sensitivity of records  Reported to ICO  Communication to patients likely  Recorded as a personal data breach |

**3. Reporting incidents**

Incidents and personal data breaches should be reported to the pharmacy IG lead (or SIRO). [Include if the IG Lead (SIRO) is not the person identified in Section 1 for staff to report incidents]

The IG lead (SIRO) will determine whether there is also a need to report the incident to others depending on the type and likely consequences of the incident, e.g. inform the ICO, data subjects, Police, NHS England, the pharmacy’s insurer etc.

**Notifying the ICO and informing the patient**

If the breach is **likely** to result in a risk to the rights and freedoms of a patient, the ICO should be informed of the breach. Notifying the ICO must be done without undue delay, and no later than 72 hours after you first become aware of the breach.

If the breach is likely to result in a **high risk** to the rights and freedoms of a patient, the patient should be informed of the breach. This is subject to certain caveats.

Currently, there is little guidance about the risks to the rights and freedoms of patients, but it is suggested that:

* if personal data is lost in a pharmacy or in a controlled environment, this is unlikely to be a risk to the rights and freedoms of patients.
* if a prescription is lost in a public place, this is likely to be a risk to the rights and freedoms of the patient.
* if there is disclosure of a patient’s medical condition to an unauthorised person, this is likely to be a high risk to the rights and freedoms of the patient.

Any notification to the ICO must describe the nature of the breach, such as numbers of data subject, records and what was lost e.g. a prescription; the name and contact details of the DPO; likely consequences of the breach; measures you have taken, for example to mitigate any adverse effect. Where any information is not possible to provide immediately, it may be provided later, but without undue delay.

Template J: Consider personal data breaches (part 2)

**(IG Template 12 updated)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Community Pharmacy Information Security Incident Report Form** | | | | | | | |
| **Reference Number:** | | Click or tap here to enter text. | **Pharmacy/Branch name:** | | | Click or tap here to enter text. | |
| **Incident details** | | | | | | | |
| **Date of incident:** | | Click or tap here to enter text. | | | | | |
| **Location of Incident:** | | Click or tap here to enter text. | | | | | |
| **Summary of Incident:**  **(State facts only and not opinions. Include details of staff involved and any contributing factors)** | | Click or tap here to enter text. | | | | | |
| **Incident Classification**  **(including (i) whether a risk to the rights and freedoms of the patient(s) is likely and (ii) if so whether that risk is high)**  **(see incident the management procedure for guidance)** | | Click or tap here to enter text. | | | | | |
| **Brief description of action already taken** | | Click or tap here to enter text. | | | | | |
| **Actions taken to prevent a reoccurrence** | | Click or tap here to enter text. | | | | | |
| **Has the IG Lead been informed?** | | **Yes**  **No** | | | **Has NHS England**  **been informed?** | | **Yes**  **No** |
| **Have you contacted your insurers?** | | **Yes**  **No** | | | **Have you sought advice from the DPO?** | | **Yes**  **No** |
| **Must you notify the ICO?** | | **Yes**  **No** | | | **Have you notified the ICO without delay and within 72 hours?** | | **Yes**  **No** |
| **Must you inform the patient(s)?** | | **Yes**  **No** | | | **Have you informed the patient(s) without delay?** | | **Yes**  **No** |
| **Details of any advice provided to pharmacy** | | Click or tap here to enter text. | | | | | |
| **Reporter details** | | | | | | | |
| **Name** | Click or tap here to enter text. | | | ***Job title (#)*** | | Click or tap here to enter text. | |
| **Information Governance Lead follow up (investigations, findings and planned actions)** | | | | | | | |
| Click or tap here to enter text. | | | | | | | |
| **IG Lead Name:** | Click or tap here to enter text. | | | ***Date*** | | Click or tap here to enter text. | |

# Template K: Think about data subject rights

**Activity: Consider the following data subject rights you may be asked about.**

|  |  |
| --- | --- |
| **Right** | **Details** |
| The right to be informed | Privacy Notice and, as appropriate, bringing the data subjects’ attention to the notice. Note requirements if personal data is received from third-parties- the data subject must be informed within a reasonable time (one calendar month) and at least on the first communication. |
| The right of access | Provide the information you hold on the data subject free of charge **within one calendar month**, unless you explain why not and possibility of lodging a complaint to the ICO. (Also, potentially other information on processing, but this is usually provided in the Privacy Notice) |
| The right to rectification | Generally, the right to rectification – correction – will not mean changing the record of medicines dispensed or other health data, but may, for example, mean correcting a name or address or adding a note of explanation to the record. You should identify those members of staff who may correct a record if requested to do so by a patient. |
| The right to erasure | Generally, this right is **not** relevant to pharmacy records; but see below the right to object. |
| The right to restrict processing | For example, while the accuracy of the data is verified by you, or to stop you destroying the record according to your pharmacy protocols, because the data subject wants you to keep it for the purposes of a legal claim. |
| The right to data portability | Generally, this right is **not** relevant to pharmacy records. This right applies only in certain circumstances, for example if lawful processing of the personal data is by consent of the data subject or a contract and is carried out by automated means. |
| The right to object | Data subjects have the right to object to you processing their data (in the performance of a task in the public interest) and if they do you will have to consider whether your need to continue processing (e.g. holding a record) overrides their interests, rights and freedoms. In most cases, you will need to retain the data according to your retention policy. The National Data Opt-Out will need to be applied when it is introduced. |
| ‘Automated decision -making’ | Generally, this right is not relevant to pharmacy records. |

Template K: Continued

**Activity: Keeping a log of data subject rights.**

You should also keep a log of those exercising their data subject rights, for example, those asking for a copy of their records, so that you can show you are complying with this part of the GDPR

|  |  |  |  |
| --- | --- | --- | --- |
| **DATA SUBJECT RIGHTS – LOG OF REQUESTS** | | | |
| **Name** | **Date of request** | **Type of right/request and information provided** | **Date completed** |
| *e.g. Mr P Smith* | *1 June 2018* | *right of access – PMR record provided* | *4 June 2018 (within one calendar month)* |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
|  |  |  |  |
|  |  |  |  |

You should seek advice if you receive a data subject request with which you are unfamiliar.

In brief, generally any personal data you collect by consent must be deleted if consent is subsequently withdrawn, with various exceptions including potential legal proceedings.

# Template L: Ensure privacy by design and default

The GDPR makes privacy by design – data protection by design and default a legal requirement, indicating that you need to implement technical and organisational measures to ensure you only process personal data necessary for the task, taking into account what you are doing with the data, how long it is being stored, the accessibility required and the risks involved given the nature and scope of the data.

Consider your use of personal data to support your pharmacy:

|  |  |  |
| --- | --- | --- |
| **Activity** | **Issues** | **Date confirmed** |
| Processing of data within the NHS for post payment verification and other related activities: | Is patient data removed from any information provided to the NHS BSA for post payment verification submissions? | Click or tap here to enter text. |
| Local commissioning | Can data be submitted in pseudonymised form? | Click or tap here to enter text. |
| Pharmacy accounts: | Is patient data removed for routine accounts work that does not need patient information? | Click or tap here to enter text. |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |

There will be other activities and other examples you can list to ensure that you process data with the minimum risk to patients, the data subjects.

# Template M: Data protection impact assessment (DPIA)

Data controllers introducing new technologies or where processing is likely to result in a **high risk** to the ‘rights and freedoms of individuals’ must carry out a DPIA.

**High risk** processing includes large-scale processing of special categories of personal data, such as healthcare data, and so includes larger community pharmacy businesses. The ICO will be introducing updated guidance on DPIAs soon, but it is suggested that for smaller community pharmacies, a DPIA is not required for current routine provision of NHS pharmaceutical services.

Where appropriate, the views of data subjects, including patients, should be sought.

|  |  |  |
| --- | --- | --- |
| **Activity** | **Comments** | **Is a DPIA required** |
| The majority of current community pharmacy practice | The processing of personal data in pharmacies is largely as a result of legal provisions in the NHS (Pharmaceutical and Local Pharmaceutical Services) Regulations 2013. | No, unless you are a national or regional community pharmacy. |
| The introduction of the Electronic Prescription Service (EPS) | The pharmacy practices and procedure are significantly different, but the pharmacy takes appropriate steps in accordance with NHS guidance to ensure the security and proper processing of electronic prescriptions. | Maybe, pharmacy practices will change, but arguably risks were assessed as part of the development of EPS. |
| The introduction of a dispensing robot | This is the introduction of new technology and is likely to result in significant changes to pharmacy practices and procedures. | Yes. |

The pharmacy DPIA should include consideration of:

* a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller;
* an assessment of the necessity and proportionality of the processing in relation to the purpose;
* an assessment of the risks to individuals;
* the measures in place to address risk, including security and to demonstrate that you comply;
* unmitigated risks (uncontrolled) have been identified and notified to the ICO; and
* a DPIA can address more than one project.

**The policies and guidance previously supporting the IG Toolkit (‘Toolkit’) are:**

Guidance about Toolkit completion: [[Toolkit](http://psnc.org.uk/ds)](https://psnc.org.uk/ds)

Template 1: [IG Policy](https://psnc.org.uk/dstemplates)

Template 2: [Staff Confidentiality Agreement](https://psnc.org.uk/dstemplates)

Template 3: [Staff Confidentiality Code](https://psnc.org.uk/dstemplates)

Template 4: [Data Handling Procedure](https://psnc.org.uk/dstemplates)

Template 5: Patient Information Leaflet **(revised version in this booklet)**

Template 6: [Asset Register](https://psnc.org.uk/dstemplates) (MS Word) / [Asset Register](https://psnc.org.uk/dstemplates) (MS Excel)

Template 7: [Physical Security Risk Assessment](https://psnc.org.uk/dstemplates)

Template 8: [Mobile Computing Guidelines](https://psnc.org.uk/dstemplates)

Template 9: [Portable equipment](https://psnc.org.uk/dstemplates) / [Asset control form](https://psnc.org.uk/dstemplates)

Template 10: [Disposal of Portable Assets](https://psnc.org.uk/dstemplates)

Template 11: Incident Management Procedures **(revised version in this booklet)**

Template 12: Information Security Incident Report Form **(revised version in this booklet)**

Template 13: [Audit Sheet](https://psnc.org.uk/dstemplates)

Template 14: [Staff Signature List](https://psnc.org.uk/dstemplates) / [Staff Signature List](https://psnc.org.uk/dstemplates) (Separate List)

Template 15: [Access Control and Password Management Procedure](https://psnc.org.uk/dstemplates)

Template 16: [Ensuring Staff Compliance with RA01 Terms Template SOP](https://psnc.org.uk/dstemplates)

*Note: These templates and guidance and the Toolkit may be further updated after the publication of this GDPR WB.*

[Emergency Planning/ Business Continuity](http://psnc.org.uk/contract-it/essential-service-clinical-governance/emergency-planning/)