

# The General Data Protection Regulation and associated legislation



## Workbook for Local Pharmaceutical Committees



**WALSALL LPC DRAFT** May 2018



## Contents

Template A: <b>D</b> ecide who is responsible.....	3
Template B: <b>A</b> ction Plan .....	4
Template C: <b>T</b> hink about and record the personal data you process; .....	5
<b>A</b> ssure your lawful basis for processing.....	5
Template D: <b>P</b> rocess according to data protection principles.....	10
Template E: <b>R</b> eview and check with your processors .....	111
Template F: <b>O</b> btain consent if you need to .....	13
Template G: <b>T</b> ell people about your processes: the Privacy Notice .....	144
Template H: <b>E</b> nsure data security.....	145
Template I: <b>C</b> onsider personal data breaches.....	188
Template K: <b>T</b> hink about data subject rights .....	22
Template L: <b>E</b> nsure privacy by design and default.....	26
Template M: <b>D</b> ata protection impact assessment (DPIA) .....	27

## Template A: Decide who is responsible

### Local Pharmaceutical Committee (LPC)

WALSALL LPC

The LPC is the data controller and is responsible/accountable for data protection and implementation of the GDPR.

### LPC Secretary/CO - responsible for GDPR compliance

Jan Nicholls

Contact Secretary via the [LPC Website](#)

### IG Lead / Senior Information Risk Owner (SIRO)

Daljit Sandhu (VC)

Contact SIRO via the [LPC Website](#)

### And potentially:

### Data Protection Officer (if applicable, which is unlikely)

Harj Sadhra

Contact DPO via the [LPC Website](#)

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.

**NB: Business data is not subject to the GDPR – but some ‘business data may also be personal data and subject to the GDPR; and, Anonymous data (e.g. statistical data) is not personal data but pseudonymised data is personal data even if you do not have the key or information to identify the data subjects.**

## Template B: Action Plan

Plan for implementation	Date achieved
Decide who is responsible	11/04/2018
Action plan	15/05/2018
Think about and record the personal data you process	15/05/2018
Assure your lawful basis for processing	15/05/2018
Process according to data protection principles (Policies)	15/05/2018
Review and check with your processors	24/05/2018
Obtaining consent if you need to	15/05/2018
Tell people about your processes: Privacy Notice	01/05/2018
Ensure data security	15/05/2018
Consider personal data breaches	15/05/2018
Think about data subject rights	15/05/2018
Ensure privacy by design and default	15/05/2018
Data protection impact assessment	15/05/2018
DPO appointed, if applicable	15/05/2018
Relevant ICO number	<b>22427101</b>
ICO fee paid annually, expires:	<b>25 November 2018</b>

**LPC Secretary has signed off the policies and procedures in this workbook and related policies and procedures**



Jan Nicholls, LPC Secretary 15/05/2018

Annual review date not later than March 31st annually

## Template C: Think about and record the personal data you process and Assure your lawful basis for processing

### Activity: records of contractors and other contacts used for the work of the LPC including NHS mail accounts

<b>LPC status</b>	Data Controller
<b>Data subjects and personal data</b>	Personal data such as name, address and contact details that may be part of business data (business data is not subject to the GDPR)
<b>Purpose</b>	LPCs must be able to communicate with their contractors as part of the wider management of the NHS
<b>Lawful basis for processing personal data</b>	Article 6(1)(f) of the GDPR. Necessary for the performance of a task in the public interest <b>or</b> Article 6(1)(f) the legitimate interests of the LPC
<b>Special category of personal data</b>	No
<b>Basis for processing special category of data</b>	N/A
<b>How is data collected?</b>	As appropriate from contractors, PSNC, NHS England, NHSBSA, Primary Care Support England, Commissioners and overarching management teams for LPCs (most such data is business data in the public domain and not subject to the GDPR, but some data may be personal data and subject to the GDPR)
<b>How is data stored?</b>	Electronically/paper
<b>How long is data stored?</b>	In line with NHS guidance for current contractors and/or connected with a contractor.  e.g. while the individual is a contractor, appropriate contact information kept for 7 years
<b>To whom do you provide the data (recipients)?</b>	As appropriate to contractors, PSNC, NHS England, NHSBSA, Primary Care Support England, Commissioners and overarching management teams for LPCs (most such data is business data in the public domain and not subject to the GDPR, but some data may be personal data and subject to the GDPR – Pharmas)
<b>Date confirmed that this applies to your LPC</b>	May 11th 2018

**NB. Much of an LPC's contractor data is likely to be business data and not personal data and, therefore, not subject to the GDPR.**

### Activity: LPC Committee Member records

<b>LPC status</b>	Data Controller
<b>Data subjects and personal data</b>	Personal data relevant to LPC service including name, address, contact details, bank details and relevant financial details, contacts and reference numbers, appraisals, contracts
<b>Purpose</b>	<del>Employment, tax and National Insurance purposes</del> -N/A
<b>Lawful basis for processing personal data</b>	Article 6(1)(e) of the GDPR, necessary for the performance of a task in the public interest <b>or</b> Article 6(1)(c) necessary for the performance of a contract
<b>Special category of personal data</b>	<del>Health data and DBS checks, as appropriate</del> N/A
<b>Basis for processing special category of data</b>	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]
<b>How is data collected?</b>	From employers and referees; job application, interview form, holiday and sick notes; appraisals and complaints against
<b>How is data stored?</b>	Paper and digital
<b>How long is data stored?</b>	Term of office or 7 years
<b>To whom do you provide the data (recipients)? (including processors)</b>	PSNC, CPWM, other LPCs, NHSE, HEE, other health-related organisations/companies as appropriate  Auditor for annual accounts  (Processors are not other data controllers to which you provide personal data, such as an employee's pension company or the HMRC or the employee's bank)
<b>Date confirmed that this applies to your LPC</b>	10th May 2018

## Template C continued

### Activity: Enhanced and other local commissioned services – data concerning health.

NB. Walsall LPC are not currently copied in to any patient/personal data for enhanced or locally commissioned services.

LPC status	Data Processor
Data subjects and personal data	Pseudonymised personal data may occasionally be processed by the LPC in the future but is currently outside our scope. If used it would <b>exclude</b> the patient name, address and contact details but <b>include</b> medicines and relevant health data  The key to identify patients <b>would not be</b> held by the LPC
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 <b>or</b> Article 6(1)(f) the legitimate interests of the LPC
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' 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?	Within PharmOutcomes and by the commissioner
How long is data stored?	Specific to the local service; details included in the service specification
To whom do you provide the data (recipients)? (including processors)	Specific to the commissioner of the service; details included in the service specification  The processor: PharmOutcomes
Date confirmed that this applies to your LPC	10/05/2018

## Template C (blank)

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

<b>Purpose</b>	Click or tap here to enter text.
<b>Lawful basis for processing personal data</b>	Click or tap here to enter text.
<b>Special category of personal data</b>	Click or tap here to enter text.
<b>Basis for processing special category of data</b>	Click or tap here to enter text.
<b>How is data collected?</b>	Click or tap here to enter text.
<b>How is data stored?</b>	Click or tap here to enter text.
<b>How long is data stored?</b>	Click or tap here to enter text.
<b>To whom do you provide the data (recipients)?</b>	Click or tap here to enter text.
<b>Date confirmed that this applies to your LPC</b>	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 retention 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 **health data** [N/A]

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 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 be GDPR compliant, your first step should be to check this or seek clarification from your processors.

Your processors may include systems used to process service data for commissioners (such as PharmOutcomes, Sonar Informatics), or any external body that undertakes your payroll for you.

List your processors and confirm any assurances sought and received:

Walsall LPC does not contract directly with any data processors with the exception of preparation of Annual Accounts. In all cases minimal relevant information is provided for data processing; that from commissioners and NHS Bodies and is generally confined to the number of interventions. Should personal information be included in future it would be pseudonymised.

Processor, product and service	Date assurances requested	Date confirmation received from processor	Date contract ends
Annual accounts: K Kaur FCCA; 348 Birmingham Road, Walsall. WS1 3NX	16/05/2018	24/05/2018	31/03/2019
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.

You may 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

NB: LPCs have a lawful basis for processing personal data because of the performance of a task carried out in the public interest or legitimate interests of the LPC (stage 1). **This should include your processing your contractor and other healthcare contacts, including NHS mail accounts, as part of, for example, the provision of information by the LPC, such as the LPC Newsletter.** (The processing of pseudonymised health data is (stage 2) for the management of health or social care systems.)

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](#).

Filing system / activity	GDPR compliant consent/explicit consent obtained	GDPR compliant consent/explicit consent recorded
Activity Click or tap here to enter text. (Date)	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: Privacy Notice

When you collect or process personal data you must provide data subjects with relevant information; the Privacy Notice. This should be available from the LPC, for example, on the LPC website; and you should draw the attention of new contractors to the Privacy Notice. A draft notice is as follows.

### WALSALL LPC PRIVACY NOTICE

#### Users of the website

The Walsall LPC website primarily exists as a resource for community pharmacists and staff.

In dealing with **Contact form** queries from the website we may have access to limited information (name, contact email address, phone, postal address) which will be handled respectfully in line with this notice. Walsall LPC do not share information with any third parties.

#### To community pharmacies

We may process your personal data (as well as your community pharmacy data), for example, your name, address, contact details (and appropriate information for payment of the statutory levy), to:

- represent and support you, as provided by the LPC constitution
- provide information to you on training events, news, services, regulatory issues, best practice and patient safety
- provide your details, as appropriate, to NHS England, NHS Business Services Authority, Primary Care Support England, Commissioners of NHS services, the Pharmaceutical Services Negotiating Committee, those who assist management of the LPC and other organisations for mutual support and advice.

We hold your information only 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 may process commercial and personal contact data in:

- performance of a task in the public interest
- provision of healthcare and treatment and for health data
- management of healthcare systems

We do not solicit or hold sensitive data on individuals.

An appropriate person is responsible for the confidentiality of data. You may object to us holding your information and may lodge a complaint with the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please ask if you want more information.

We may process limited patient health information as part of locally commissioned services carried out by community pharmacies, to assist with:

- data management
- collating limited health data (no patient names are identified in this data) from community pharmacies
- providing data to the commissioner or the person paying for the service, for example NHS England or a Local Authority

The health data are shared only with the service commissioner, not with third parties

## 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 information available for community pharmacies should be considered and equivalent policies adopted, as appropriate, by LPCs to ensure the physical, electronic and human security of personal data.

You also need to ensure data quality.

Security issues	Measures	Date measures confirmed
Physical	<p>The following existing policies for community pharmacies should be considered and adopted as appropriate:</p> <p>Template 6: <a href="#">Asset Register</a> attached</p> <p>Template 7: <a href="#">Physical Security Risk Assessment</a> not applicable – no premises</p>	09/05/2018
Electronic	<p>The following existing policies for community pharmacies should be considered and adopted as appropriate:</p> <p>Template 8: <a href="#">Mobile Computing Guidelines</a> attached</p> <p>Template 9: <a href="#">Portable equipment / Asset control form</a></p> <p>NB LPC owns no portable devices. Members are also responsible for data security on their personal equipment.</p> <p>Template 10: <a href="#">Disposal of Portable Assets</a> n/a – LPC owns no portable devices, the template will be reviewed if/when such equipment is in use.</p> <p>A risk assessment has been completed for all electronic systems used by the LPC secretary. These are for her exclusive use and are securely locked away when not in use.</p> <p>The standards of NHS mail are laid out within user agreements, and further practical considerations are listed at <a href="#">PSNC's NHSmail webpage</a>. 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.</p>	09/05/2018

	<p>Fax machines should only be used to send sensitive data as a very last resort and, when used, staff should consider local <a href="#">“Safe Haven” procedures</a>. Fax numbers should be checked and verified before confidential information is sent to them. n/a – not used for LPC business</p> <p>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.</p> <p>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.</p> <p>Carefully consider the <a href="#">“Ten steps to help improve data and cyber security within your pharmacy”</a> briefing document which includes further information about electronic data security and the extent to which these may apply to the LPC.</p>	
Human	<p>The following existing policies for community pharmacies should be considered and adopted as appropriate:</p> <p>Template 2: <a href="#">Staff Confidentiality Agreement</a></p> <p>Template 3: <a href="#">Staff Confidentiality Code</a></p> <p>(Staff monitoring of access to personal data is also required)</p> <p>Template 4: <a href="#">Data Handling Procedure</a></p> <p>Template 13: <a href="#">Audit Sheet</a></p> <p>Template 14: <a href="#">Staff Signature List / Staff Signature List (Separate List)</a></p> <p>Template 15: <a href="#">Access Control and Password Management Procedure</a></p> <p>Template 16: <a href="#">Ensuring Staff Compliance with RA01 Terms Template SOP</a></p>	Click or tap here to enter text.

LPCs may need to rely on appropriate experts to provide the relevant technical assurances, for example, 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. Any personal data breaches may result in a review of policies and a review of the incident management procedures.

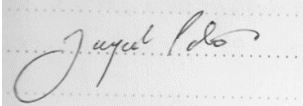
## DATA QUALITY



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.

<b>Activity</b>	<b>LPC officers and members</b>
Adding information	Secretary, Treasurer
Amending information	Secretary, Treasurer
Deleting information	Secretary, Treasurer
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)

WALSALL LPC				
<b>Information Security Incident Management Procedures</b>				
Procedures Prepared by: LPC Secretary	Procedures Approved by:  Chair, Walsall LPC	Date Next Review Due:	31/03/2019	
Date Prepared: 11/05/2018	Date Approved: 15/05/2018	Date Review Takes Place:	31/03/2019	

*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 suspicious incidents should be reported to LPC secretary

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 Secretary/Chair/Governance Group

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 personal data 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 or an LPC member)

- 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 data confidentiality, by a member of the public or LPC member:

- 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 person(s) as appropriate
- Categorise and report the incident as described as per 'recording and reporting' requirements.

E) Loss of data in transit.

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

### 3. Reporting incidents

Incidents and personal data breaches should be reported to the LPC CO.

The LPC CO 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 LPC insurer (contact PSNC for details if relevant) etc.

#### Notifying the ICO and informing the data subject

If the breach is **likely** to result in a risk to rights and freedoms, 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 rights and freedoms eg a community pharmacy contractor, the data subject 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 which may be compromised, but it is suggested that:

- if contractor personal data is lost, this is unlikely to be a risk to rights and freedoms;
- if there is disclosure of contractor personal data to an unauthorised person, this is likely to be a high risk to their rights and freedoms.

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. personal data; the name and contact details of the DPO (if applicable); 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.

## Consider personal data breaches (part 2)

**(IG Template 12 updated)**

**WALSALL LPC Information Security Incident Report Form**

<b>Reference Number:</b>	Click or tap here to enter text.	<b>LPC:</b>	Click or tap here to enter text.
--------------------------	----------------------------------	-------------	----------------------------------

**Incident details**

<b>Date of incident:</b>	Click or tap here to enter text.
--------------------------	----------------------------------

<b>Location of Incident:</b>	Click or tap here to enter text.
------------------------------	----------------------------------

<b>Summary of Incident:</b> (State facts only and <u>not</u> opinions. Include details of LPC members involved and any contributing factors)	Click or tap here to enter text.
---	----------------------------------

<b>Incident Classification</b> (including (i) whether a risk to rights and freedoms 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.
--	----------------------------------

<b>Brief description of action already taken</b>	Click or tap here to enter text.
--	----------------------------------

<b>Actions taken to prevent a reoccurrence</b>	Click or tap here to enter text.		
<b>Has the IG Lead been informed?</b>	Yes <input type="checkbox"/>	<b>Has NHS England been informed?</b>	Yes <input type="checkbox"/>
	No <input type="checkbox"/>		No <input type="checkbox"/>
<b>Have you contacted your insurers?</b>	Yes <input type="checkbox"/>	<b>Have you sought advice from the DPO (if applicable)?</b>	Yes <input type="checkbox"/>
	No <input type="checkbox"/>		No <input type="checkbox"/>
<b>Must you notify the ICO?</b>	Yes <input type="checkbox"/>	<b>Have you notified the ICO without delay and within 72 hours?</b>	Yes <input type="checkbox"/>
	No <input type="checkbox"/>		No <input type="checkbox"/>
<b>Must you inform the patient(s)?</b>	Yes <input type="checkbox"/>	<b>Have you informed the patient(s) without delay?</b>	Yes <input type="checkbox"/>
	No <input type="checkbox"/>		No <input type="checkbox"/>
<b>Details of any advice provided to LPC</b>	Click or tap here to enter text.		
<b>Reporter details</b>			
<b>Name</b>	Click or tap here to enter text.	<b>Job title (#)</b>	Click or tap here to enter text.
<b>LPC CO (investigations, findings and planned actions – it may be advisable to report all data breaches to the LPC and ensure they are recorded in the minutes of the meeting)</b>			
Click or tap here to enter text.			
<b>LPC CO Name:</b>	Click or tap here to enter text.	<b>Date</b>	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. <b>If the data is pseudonymised and you do not have access to the patient information you do not have to do this.</b>
The right of access	Provide the information you hold on the data subject free of charge <b>within one calendar month</b> , 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). <b>Generally, you cannot provide information on request if the data subject is not identified in the data (the data is pseudonymised).</b>
The right to rectification	For the LPC, the right to rectification – correction – should be straightforward for contractor data and generally will not be applicable to pseudonymised data.
The right to erasure	This may be applicable to contractor personal data (not business data) and generally will not be applicable to pseudonymised data.
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 LPC 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 <b>not</b> relevant to LPCs. 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 although this is unlikely to apply to LPCs.
'Automated decision -making'	Generally, this right is not relevant to LPC records.

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
<i>e.g. Mr P Smith</i>	<i>1 June 2018</i>	<i>right of access – contractor record provided</i>	<i>4 June 2018 (within one calendar month)</i>
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 J: 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 LPC:

Activity	Issues	Date confirmed
Processing of data to support locally commissioned services	In the unlikely event <b>patient data</b> is included - is it <b>pseudonymised</b> ?	Click or tap here to enter text.
LPC pay and accounts:	Is any <b>member data removed</b> for routine accounts work that does not need such information eg annual accounts?	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 LPC members or officers and community pharmacy contractors; the data subjects.

## Template K: 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, but this **is unlikely to apply to LPCs**. The ICO will be introducing updated guidance on DPIAs soon.

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

A 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 previously supporting **community pharmacies** to complete the IG Toolkit are:**

1: [IG Policy](#) ✓

Template 2: [Staff Confidentiality Agreement](#) ✓

Template 3: [Staff Confidentiality Code](#) ✓

Template 4: [Data Handling Procedure](#) ✓

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

Template 6: [Asset Register](#) (MS Word) ✓

Template 7: [Physical Security Risk Assessment](#) ✓

Template 8: [Mobile Computing Guidelines](#) ✓

Template 9: [Portable equipment / Asset control form](#) ✓

Template 10: [Disposal of Portable Assets](#) ✓

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](#) ✓

Template 14: [Member Signature List](#) ✓

Template 15: [Access Control and Password Management Procedure](#) ✓

Template 16: [Ensuring Staff Compliance with RA01 Terms Template SOP](#) ✓

[Emergency Planning/ Business Continuity](#) ✓

**Where appropriate policies have been adapted or substituted to support LPC work.**

**The policies supporting Walsall LPC compliance with GDPR are:**

[Code of Conduct and Confidentiality Agreement](#)

[Committee Member Details and Declaration of Interests](#)

[Asset Register](#)

[Mobile Computing Guidelines](#)

[IG Policy](#)

[Data Handling Procedures](#)

[Continuity and Succession Plan](#)