# The General Data Protection Regulation and associated legislation for Community Pharmacy Hertfordshire

# Contents

# Template A: Decide who is responsible

**Community Pharmacy Hertfordshire**

Community Pharmacy Hertfordshire (CPH) is the data controller and is responsible and accountable for data protection and implementation of the GDPR.

| | |
|---|---|
| **Officer responsible for GDPR compliance** | **Business Officer** |
| **IG Lead / Senior Information Risk Owner (SIRO)** | **Chief Officer** |
| **Data Protection Officer**<br>The DPO may, or may not, be a member of staff.<br><br>Confirmed by: ICO DPO requirement | **N/A** |

**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 (eg. 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 | 01/09/25 |
| Action plan | 01/09/25 |
| Think about and record the personal data you process | 01/09/25 |
| Assure your lawful basis for processing data | 01/09/25 |
| Process according to data protection principles (Policies) | 01/09/25 |
| Review and check with your processors | 01/09/25 |
| Obtaining consent if you need to | 01/09/25 |
| Tell people about your processes: the Privacy Notice | 01/09/25 |
| Ensure data security | 01/09/25 |
| Consider personal data breaches | 01/09/25 |
| Think about data subject rights | 01/09/25 |
| Ensure privacy by design and default | 01/09/25 |
| Data protection impact assessment | 01/09/25 |
| | |
| DPO appointed (if applicable) | N/A |
| Relevant ICO number | Z2205944 |
| Paid current annual fee to the ICO | 05/04/25 |

**Community Pharmacy Hertfordshire has signed off the policies and procedures in this workbook and related policies and procedures**

Chief Officer 01/09/25

Signed:

Review date: 01/09/28

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

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

| LPC Status | Data Controller |
|---|---|
| **Data subjects and personal data** | Personal data such as name, address and contact details that may be part of business data (business data is not subject to the GDPR). |
| **Purpose** | CPH must be able to communicate with their contractors as part of the wider management of the NHS. |
| **Lawful basis for processing personal data** | Article 6(1)(e) GDPR. Necessary for the performance of a task carried out in the public interest **or** Article 6(1)(e) the legitimate interests of CPH. |
| **Special category of personal data** | No (financial data does not raise the same fundamental issues and so does not constitute special category data for the purposes of the GDPR). |
| **Basis for processing special category of data** | N/A |
| **How is data collected?** | As appropriate from contractors, CPE, NHS England, PCSE, NHSBSA, commissioners and overarching management teams for CPH (most 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). |
| **How is data stored?** | Cloud based server, PharmOutcomes, Mailchimp, Sage, Google Analytics, Pomroy Associates, Tristar, Airtable, PDFgear. |
| **How long is data stored?** | Up to 7 years from end of employment/contract. |
| **To whom do you provide the data (recipients)?** | As appropriate to contractors, CPE, NHS England, PCSE, NHSBSA, commissioners and overarching management teams for CPH (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). |
| **Date confirmed that this applies to CPH** | 01/09/25 |

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

## Activity: Employment records

| CPH Status | Data Controller |
|---|---|
| **Data subjects and personal data** | Personal data relevant to employment including employee name, address, contact details, bank details and relevant financial information, contacts and reference numbers, staff appraisals, contracts, pension. |
| **Purpose** | Employment including tax and National Insurance. |
| **Lawful basis for processing personal data** | Article 6(1)(e) of the GDPR, necessary for the performance of a task in the public interest **or** Article 6(1)(c) necessary for the performance of a contract. |
| **Special category of personal data** | No |
| **Basis for processing special category of data** | N/A |
| **How is data collected?** | From employees and referees, job application, interview form, holiday and sick notes, appraisal data and work conduct issues. |
| **How is data stored?** | Cloud based server. |
| **How long is data stored?** | 7 years |
| **To whom do you provide the data (recipients)?**<br>**(including processors)** | Sage, Pomroy Associates, People's Pension, Cloud based server, Business Officers on behalf of CPH, Tristar. |
| **Date confirmed that this applies to CPH** | 01/09/25 |

# Template C continued

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

| CPH Status | Data Processor |
|---|---|
| **Data subjects and personal data** | On occasion, personal data may be received.<br>Pseudonymised personal data that **excludes** the patient name, address and contact details but **includes** medicines and relevant health information.<br>The key to identify patients **is not** held by CPH. |
| **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 **or** Article 6(1)(f) the legitimate interests of CPH. |
| **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).<br>'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?** | PharmOutcomes or Cloud based server. |
| **How long is data stored?** | Specific to the local service and evaluation data kept indefinitely by external parties. |
| **To whom do you provide the data (recipients)? (including processors)** | Specific to the commissioner of the service - details included in the service specification.<br>The processor is currently PharmOutcomes. |
| **Date confirmed that this applies to CPH** | 01/09/25 |

# Retention of records

The following may be helpful in considering retention periods. As part of CPH authority we must be aware of the rights and requirements for data retention of records in line with community pharmacy.

For further guidance and information on retaining pharmacy records please visit the Specialist Pharmacy Service (SPS) website for the latest information - *Retention of Pharmacy Records*

Patient records may be retained longer than the minimum retention period and this should be in line with the workbook included in Template C. **(NB. this is for pharmacy reference only if you are required to provide guidance).**

# 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: Under statute, common law (including duty of care) or legal proceedings.
- Overriding public interest: 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.*

# 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 can be found in the link provided.

Following the data protection principles involves for example:

| **Principle** | **Issues to consider** |
|---|---|
| Lawfully | All your processing is lawful (templates C and F).<br>Responsibilities, SIRO, 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 (templates G, I, J and K).<br>Processors' contracts are appropriate (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 (templates L and M).<br>Processors' contracts are appropriate (template E). |
| Accurate/up to date | Records are accurate and, if relevant, up to date (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 (template L). |
| Security | There is appropriate physical, electronic and human security (template H). |
| Integrity | Data is backed up so that it is protected against accidental loss or damage (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 or Sage), or any other external body that undertakes systems on behalf of CPH.

List your processors and confirm any assurances sought and received.

| **Processor, product and service** | **Date assurances requested** | **Date contract ends** |
|---|---|---|
| Google Analytics | 18/9/25<br>https://business.safety.google/privacy/ | Ongoing |
| Sage | 18/9/25<br>https://www.sage.com/en-gb/legal/privacy/ | Ongoing |
| Mailchimp | 18/9/25<br>https://mailchimp.com/help/about-the-general-data-protection-regulation/ | Ongoing |
| PharmOutcomes | 18/9/25<br>https://pharmoutcomes.org/pharmoutcomes/help/home?privacypolicy | Ongoing |
| Tristar | 18/9/25<br>https://tristarwebsolutions.co.uk/gdpr-request-personal-data/ | Ongoing |
| Pomroy Associates | 18/9/25<br>https://www.pomroyassociates.co.uk/privacy-policy | Ongoing |

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: CPH 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 CPH (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 CPH, such as the CPH 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, 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 ie. 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 ICOs guidance on consent.

| **Filing system / activity** | **GDPR compliant consent/explicit consent obtained** | **GDPR compliant consent/explicit consent recorded** |
|---|---|---|
| Activity<br>Click or tap here to enter text.<br>*(Date)* | Consent obtained on<br>Click or tap here to enter text.<br>*(Date)* | Consent recorded in<br>Click or tap here to enter text.<br>*(Name filing system/computer)* |
| | | |
| | | |

Template G: Tell people about your processes: Privacy Notice

# Privacy Notice

## Who We Are

Community Pharmacy Hertfordshire (CPH)
Unit 27b Weltech Centre, Ridgeway, Welwyn Garden City, AL7 2AA

This Privacy Notice explains how Community Pharmacy Hertfordshire (CPH) collects, uses, and protects your personal data. We are committed to transparency and ensuring your privacy is respected.

## The Data We Collect and Why

We collect and process different types of personal data depending on whether you are a community pharmacy or a patient.

**For Community Pharmacies**
We process your personal data (and your pharmacy business data) to **represent and support you**, as outlined in the LPC Constitution. This includes information like your name, address, contact details such as mobile number and email address, and appropriate information for payment of the levy.

This section details how we handle information related to:

**Pharmacy Contractors (Business & Levy Information)**
We collect and process data related to **pharmacy contractors and their businesses** for purposes such as:

**Levy Management:** Your name, address, contact details, and other appropriate information are used for the payment and management of the levy.
**Information Sharing for Mutual Support:** We may provide your business details (e.g., pharmacy name, address, and primary contact information) to organisations such as NHS England, NHS Business Services Authority, Primary Care Support England, commissioners of NHS services, Community Pharmacy England, those who assist in the management of the LPC, and other relevant organisations for mutual support, advice, and to provide you with important information. This includes details on training events, news relevant to contractors, service updates, regulatory information, best practice guidelines and important deadlines.

**Community Pharmacy Staff (Personal Data)**
We may also hold **personal data for a number of community pharmacy staff members** (e.g., names, roles, and contact details for training or communication purposes, where provided directly to us).
**Crucially, we will never share the personal data of individual community pharmacy staff members with any third party without their explicit permission.** This personal

data is used solely for the purpose for which it was provided (e.g., to register for training, receive direct communications, or for specific projects with consent).

**For Patients**
When community pharmacies provide services, we process limited patient health information. We do this to assist with payment and service management.

We collate limited health data from community pharmacies. Please note that patient names are not identified in this data.
This anonymised data is provided to the commissioner of the service, such as NHS England or a local authority, for payment or service management purposes.
We only share this limited health data with the service commissioner and other parties explicitly identified during the service's consent process.

## Our Legal Basis for Processing Your Data

We process your personal data because it is necessary for the performance of a task carried out in the public interest. This includes the provision of healthcare and treatment, and for health data, the management of healthcare systems.

An appropriate person within CPH is responsible for ensuring the confidentiality of your health data.

## Your Rights

You have important rights regarding your personal data:

**Right to Access:** You have the right to request a copy of the information we hold about you, free of charge.
**Right to Rectification:** You can ask us to correct any inaccurate information we hold about you.
**Right to Object:** You have the right to object to us holding or processing your information.

## How Long We Keep Your Data

We retain your information for as long as advised by our retention guidelines that follow national statutory and regulatory requirements.

## How to Contact Us or Make a Complaint

If you have any questions, want more information, or wish to exercise your rights, please contact CPH:

**Email:** info@cpherts.org.uk **Telephone:** 01707 390095

If you are not satisfied with our response to your complaint, you can escalate the matter to:
**The Information Commissioner's Office (ICO)**: https://ico.org.uk/.

**June 2025**

# 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 CPH to ensure the physical, electronic and human security of personal data.

| **Security issues** | **Measures (templates available on CPE website)** | **Date measures confirmed** |
|---|---|---|
| Physical | The following existing policies for CPH should be considered and adopted as appropriate:<br><br>- Asset register<br>- A completed physical Security Risk assessment | 01/09/25 |
| Electronic | The following existing policies for CPH should be considered and adopted as appropriate:<br><br>**Templates to consider**<br><br>- Mobile computing guidelines<br>- Portable equipment register<br>- Disposal of portable assets<br><br>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 can assist with this (Tristar).<br><br>**Staff awareness training –** eg. 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. | 01/09/25 |
| Human | The following existing policies for CPH should be considered:<br>- Staff confidentiality agreement.<br>- Access control and password management procedures. | 01/09/25 |

CPH will need to rely on appropriate experts to provide the relevant technical assurances, for example, Tristar or others providing technical support and ensure you comply with the technical standards.

Review of data security policies and practices will be performed annually, in line with CPE advice.

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.

| **Activity** | **Staff names or groups of staff** |
|---|---|
| Adding information contractors | All staff |
| Amending information contractors | All staff |
| Deleting information contractors | All staff |
| HR information – personal data | Chief Officer and Business Officer |

# Template I: Consider personal data breaches

| | | | | |
|---|---|---|---|---|
| Community Pharmacy Hertfordshire<br><br>**Information Security Incident Management Procedures** | | | | |
| **Procedures prepared by:**<br>Business Officer | **Procedures approved by:**<br>Chief Officer | **Date next review due:** | 01/09/28 | |

*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 the Business Officer.

Incidents should always be investigated immediately whilst there is still the possibility of collecting as much evidence as possible. Investigations should normally be coordinated between at least two individuals (Business Officer or Chief Officer).

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 eg. 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):
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 (eg. disciplinary, advice/training, contractual).

d) Procedure for dealing with complaints about data 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 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 (eg. 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 risk to rights as highlighted by CPE)** | **Major: (consider whether likely to result in a high risk to rights as highlighted by CPE)** | **Critical: (likely to result in a high risk to rights as highlighted by CPE)** |
|---|---|---|---|---|
| Minimal risk - indiscernible effect on data subjects | Minor breach – eg. data lost but files encrypted, less than 5 data subjects affected | Moderate breach – eg. unencrypted records lost, up to 20 data subjects affected | Serious breach – eg. unencrypted records lost, **up to 1,000 data subjects** affected or particular sensitivity | Serious breach in terms of volume of records – eg. **over 1,000 data subjects** 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 Chief Officer.

The Chief Officer will determine whether there is also a need to report the incident to others depending on the type and likely consequences of the incident, eg. inform the ICO, data subjects, Police, NHS England, CPH insurer (contact CPE for details if relevant) etc.

### Notifying the ICO and informing the data subject

If you believe the breach to be moderate to critical please consult the ICO website for further guidance.

# Template J: Consider personal data breaches (part 2)

| **Community Pharmacy Hertfordshire Information Security Incident Report Form**<br>**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:**<br>**(state facts only and not opinions. Include details of staff involved and any contributing factors)** | Click or tap here to enter text. |
| **Incident classification**<br>**(including (a) whether a risk to the rights and freedoms of the patient(s) is likely and (b) if so whether that risk is high)**<br>**(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 Chief Officer been informed?** | **Yes** ☐ **No** ☐ | **Has NHS England been informed? (if required)** | **Yes** ☐ **No** ☐ |
| **Have you contacted your insurers?** | **Yes** ☐ **No** ☐ | **Have you informed affected individuals?** | **Yes** ☐ **No** ☐ |
| **Must you notify the ICO?** | **Yes** ☐ **No** ☐ | **Have you notified the ICO without delay and within 72 hours?** | **Yes** ☐ **No** ☐ |
| **Details of any advice provided by the Chief Officer** | 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. |
| **Chief Officer (investigations, findings and planned actions – it may be advisable to report all data breaches to CPH and ensure they are recorded in the minutes of the meeting)** | | | |
| **Chief Officer 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. If data request refused, removal in a timely fashion. |
| 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). **Generally, you cannot provide information on request if the data subject is not identified in the data.** |
| The right to rectification | For CPH, the right to rectification "correction" should be straightforward: correction of contractor data and contact details and will not be applicable to pseudonymised data. |
| The right to removal | This may be applicable to contractor personal data (not business data) and will not be applicable to pseudonymised data. |
| The right to restrict processing | Accuracy of the data is verified by data processors, to stop individuals destroying records as per CPH protocols. Data subjects must keep data for the purposes of a legal claims (up to 7 years). |
| The right to data portability | This right applies only in certain circumstances to CPH - please check ICO website for these instances. |
| The right to object | Data subjects have the right to object to you processing their data if they do you will have to consider whether your need to continue processing. For further information please visit ICO website. |
| Automated decision making | Mailchimp and the CPH website have applicable GDPR policies in place to protect individuals in this regard. |

# 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** |
| *eg. Mr P Smith* | *1 June 2018* | *right of access – contractor 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

This is a reference for information with regard to GDPR 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 CPH.

| **Activity** | **Issues** | **Date confirmed** |
|---|---|---|
| Processing of data support locally commissioned services | Is patient data pseudonymised? | Click or tap here to enter text. |
| CPH finance and accounts | Is any employee data removed for routine accounts work that does not need such 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 employees or 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, but this **is unlikely to apply to CPH**.

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.

# Template N: CPE guidance materials

## CPE GDPR Guidance and Policy references:

There is a 13-step additional guidance available on CPE website.

For further information on data security and documentation templates, please visit CPE GDPR Data Security Templates

**For any further guidance please contact the Chief Officer.**