GDPR, revalidation, FMD and the interim quality payments scheme

Hollie Ryder
Specialist Support Pharmacist
National Pharmacy Association

Aims and objectives

- **General Data Protection Regulation (GDPR)**
  - What is GDPR, when will it be implemented and what are pharmacies required to do?
- **Revalidation**
  - What is the new framework, who is affected and when will it be implemented?
- **Falsified Medicines Directive (FMD)**
  - What is FMD, when will it be implemented and what are pharmacies required to do?
- **Quality payments scheme – June review point**
  - Update on the interim quality payments scheme

General Data Protection Regulation (GDPR)

Data protection law: what is changing?

EU Data Protection Directive → **General Data Protection Regulation (GDPR)**

(Applies from 25 May 2018)

+

Data Protection Act 1998 (DPA) → **Updated Data Protection Act**

(The Data Protection Bill is currently passing through UK parliament)

GDPR: brief overview

- Effective from **25 May 2018**
- Many concepts and principles similar to existing DPA
- **New elements** and **significantly enhanced** requirements
- GDPR is being brought to the attention of the general public

GDPR: brief overview

Key changes include:

- Updated data protection principles
- Updated conditions for processing data
- New rules regarding consent
- Enhanced data subject rights
- New, specific legal responsibilities for organisations processing children's data
- New obligations for data controllers and processors
- New addition of the '***accountability principle***' and the role of the '***Data Protection Officer***'
- Greater regulation and enforcement

Data Protection Act	The General Data Protection Regulation
Only applicable in UK	Applies to all EU countries
No requirement for a data protection officer (DPO)	Appointment of a data protection officer (DPO) required for certain organisations
Consent: does not necessarily require positive opt-in	Consent: must be specific, positively opted-in and not implied
Covers personal data and sensitive personal data	Covers personal data and special categories of data (which includes genetic/biometric data, location data and online identifiers)
Responsibility lies predominantly with the data controller	Responsibility lies with both the data controller and processor
Comparably less accountability	Accountability principle explicitly defined
Subject access request: £10 and within 40 days	Subject access request: free of charge and within 30 days

Data controllers and data processors

- The GDPR applies to all data controllers and data processors
- A **data controller** determines how and why personal data is processed - under the GDPR, the pharmacy organisation is a data controller
- A **data processor** carries out processing on behalf of the data controller –
  - Note; all individuals within a pharmacy organisation are acting as data controllers and not data processors

GDPR: data protection principles

The **six data protection principles** identified under the GDPR state that personal data **must be**:

1. *Processed lawfully, fairly and transparently*
2. *Collected for specified, explicit and legitimate purposes*
3. *Adequate, relevant and limited to what is necessary in relation to the purposes of processing*
4. *Accurate and where necessary, kept up to date*
5. *Kept in a form which allows the identification of a data subject for no longer than is necessary*
6. *Processed in a manner that ensures appropriate security*

GDPR: accountability principle

- Aim: to **minimise risk** of data breaches and promote protection of personal data
- Organisations are required to implement comprehensive **governance** measures, which must be proportionate to their processing
- It is the organisation's responsibility to ensure they are able to **demonstrate compliance**

GDPR: demonstrating compliance

- **Implement** appropriate technical and organisational measures
- Maintain **relevant documentation** on processing activities
- Appoint a **Data Protection Officer (DPO)**
- Use **data protection impact assessments (DPAI)** (where appropriate)

GDPR: data protection officer (DPO)

- DPO is required if an organisation carries out '***large scale processing of special categories of data***'
  - 'Special category data' includes health data
- **No training** is required for the role of a DPO
- However, the DPO is expected to have adequate knowledge of data protection law
- ICO have stated that the DPO can be an **existing employee** of an organisation
  - Professional duties should be compatible with DPO duties and no conflicts of interests

GDPR: records of processing activities

- Organisations processing '**special categories**' of personal data **must** maintain records of data processing activities
- Keep **up-to-date** written records of data processing activities
- Document and review regularly to demonstrate compliance
  - Why personal data is being processed
  - Description(s) of data being processed
  - Retention periods of the data

GDPR: relevant records and documents

- Records of **processing**
- **Privacy notice**
- Records of **consent**
- **Location** of personal data within the organisation
- **Contracts** between controllers and processors
- Records of **data breaches**

GDPR: lawful basis for processing

1. Data subject provides **consent** to the processing of their personal data for one/more specific purposes

2. Data processing is necessary due to a **contract** in place or prior to entering into a contract

3. Data processing is necessary for compliance with a **legal obligation** to which the controller is subject

4. Data processing is necessary to **protect** the vital interests of the data subject /another natural person

5. Data processing is necessary for the **performance of a task** undertaken in public interest or to exercise of official authority vested in the controller

6. Data processing is necessary for the **controller/third party legitimate interests**; except where the data subject's rights and freedoms overrides it, particular if the data subject is a child

GDPR: lawful basis for processing

Dispensing a prescription

- A patient effectively implies consent to enable the pharmacy to process their personal data for the purpose of dispensing a prescription
- Lawful basis: *processing is necessary for the* ***performance of a task carried out in the public interest or in the exercise of official authority vested in the controller***

Deliveries of dispensed items

- This service does not fall under the pharmacy contract consent; is required to enable a pharmacy to use an individuals personal data for the purposes of a delivery
- Lawful basis: *the data subject has given* ***consent to the processing of his or her personal data for one or more specific purposes***

GDPR: consent

- May **not always be required** – remember there are **five other lawful bases** permitting the processing data
- Must be obtained where another lawful basis for data processing is **not applicable**

Must be	Cannot be
Given **freely**, be **specific**, **informed** and **unambiguous**	Assumed from the individual's lack of action/response
Obtained by **clear affirmative action**	Through pre-ticked consent boxes
Verifiable and **positively opted-in**	Obtained by default or by using opt-out boxes
Straightforward to **withdraw consent**	Part of any terms and conditions of a service

GDPR: individual rights

- The rights of individuals under the GDPR are **similar** to those under the DPA; however, there are notable **enhancements**
- The GDPR provides **eight rights** for individuals
- Not all of the rights are absolute – some rights are only applicable in **certain circumstances**

GDPR: individual rights

1. The right to be **informed**
2. The right of **access**
3. The right to **rectification**
4. The right to **erasure**
5. The right to **restrict processing**
6. The right to **data portability**
7. The right to **object**
8. Rights in relation to **automated** decision making

GDPR: individual rights

Right to be informed

- Organisations must provide "*fair processing information*" - usually in the form of a **privacy notice**
- Privacy notice must be **concise**, **transparent**, **intelligible**, and use **clear** and **plain language**

Right of access

- Often termed a "subject access request"
- The organisation must **verify identity** of the person making the request
- Individuals have the right to:
  1. **Access** their personal data
  2. **Confirm** that their personal data is being processed
  3. **Obtain** other supplementary information

GDPR: individual rights

Right to rectification

- An individual is able to request rectification if data is:
  1. **Inaccurate**
  2. **Incomplete**
- Third party notification is required (in certain circumstances)

Right to erasure

- "**Right to be forgotten**" – permits an individual to request **deletion** of their personal data
- Individuals **do not have absolute right** – only applicable in certain circumstances
- A request to erase an individual's data can be **rejected**, if at least one of the valid reasons is met

GDPR: individual rights

Right to restrict processing

- Individuals can request for processing of their data to be **blocked – only in specific situations**
- Organisations are permitted to store the individual's data, but they are **not able to further process** it

Right to data portability

- Data portability enables individuals to **move, copy or transfer their data** in a safe and secure manner
- To comply, an organisation must provide information **free of charge,** "*in a structured, commonly used and machine-readable format*"

GDPR: individual rights

Right to object

- An individual is able to **object** to having their personal data processed **in certain circumstances**
- The right to object must be highlighted in the organisation's **privacy notice**

Rights in relation to automated decision making

- An individual should not be subject to decision making which is solely based on **automated processing** including profiling

GDPR: complying with an individual's request to exercise their right

- Take reasonable steps to **verify the identity** of the individual
- Comply without undue delay and within **specified time frames (one month)**
- Organisations must provide the information **electronically**, where possible
- Provide the information **free of charge**

GDPR: data breaches

- A personal data breach means a **breach of security leading to the destruction**, **loss**, **alteration**, **unauthorised disclosure of**, or **access** to personal data

- Organisations must **report** certain **data breaches** to the ICO
  - Breaches must be reported within **72 hours**
  - Fine dependent on infringement; up to either:
  - **€10million or 2%** of the organisation's global turnover or
  - **€20million or 4%** of the organisation's global turnover
- In some cases, contact the **affected individual(s)**, **NHS England**, **regulatory body** or **police**

GDPR: data breaches

- A personal data breach includes:
  - **Loss/theft** of personal data
  - **Sending** personal data (such as medicines with patient name/address) to an incorrect recipient
  - **Altering** patient information without consent
  - **Unauthorised** individuals accessing patient information from a PMR

GDPR: how to prepare

- **Raise awareness** within your organisation of the forthcoming changes
- Ensure individuals familiarise themselves with, and are aware of, the **six lawful bases for processing personal data** under the GDPR
- **Identify** your organisation's **lawful basis** for processing personal data
- Look into appointment of a **DPO**

GDPR: how to prepare

- **Consent**
  - Check **current and existing procedures** for obtaining consent –includes how consent is sought and recorded
  - Consider the **services offered** which require consent to process data
    - Including prescription delivery service or a repeat prescription management service, sending emails/text messages, nominating patients for EPS and accessing SCR
  - Be aware that inappropriate or invalid consent is **not** a lawful basis for processing personal data

GDPR: how to prepare

- **Individual rights**
  - Ensure individuals are aware of the **eight rights of individuals**
  - Be aware of the **time frames** the organisation needs to comply with an individual's requests
  - Review and update the **privacy notice**

- **Data breaches**
  - Review and update your organisation's procedure on managing **data breaches** to comply with the GDPR

GDPR: how to prepare

- **Data breaches**
  - Check **areas** where a data breach may occur
  - Be **aware** of, and **recognise** what is considered to be a data breach
  - **Allocate** an individual the **responsibility** of managing breaches
  - Ensure a robust system is in place for **detecting and investigating** breaches
  - Be aware when a breach needs to be **reported**
  - **Document** all data breaches within the organisation

GDPR: how to prepare

- **Relevant records and documents**
  - Perform an **audit** or **data-mapping exercise** in the pharmacy to identify data processing procedures
  - Begin to **review** agreements, contracts, policies and procedures on data sharing, retention and security; both **within the pharmacy** and with **external organisations**
  - Ensure the pharmacy has the required **up-to-date** written **records/documentation** in place

GDPR: NPA support

- Any concerns in regards to GDPR, email NPA Cheif Pharmacist, Leyla Hannbeck: L.hannbeck@npa.co.uk

National Pharmacy Association

General Data Protection Regulation (GDPR)

PHARMACY TEAM TRAINING MANUAL

Disclaimer:
As the information and guidance on the General Data Protection Regulation (GDPR) is constantly being updated, the contents of this training manual and any supporting resources may be subject to change. The information published is, to the best of our knowledge, correct at the time of publication. However, no responsibility will be accepted for any consequences of decisions made using this information.

Welcome

This staff training manual has been produced by the NPA Pharmacy team to enable members of the pharmacy organisation gather an adequate understanding of the upcoming General Data Protection Regulation (GDPR).

The GDPR aims to standardise and simplify data protection rules and strengthen individuals' rights in relation to their personal data.

A fundamental requirement for GDPR implementation is staff awareness. Pharmacy staff must have an understanding about the GDPR, its principles, and the roles, responsibilities and processes of organisations.

How to use this training manual

This training manual will help you understand the basis of the new regulation, and more importantly, provide you with information to help ensure compliance with the GDPR.

This training manual has been divided into the four following sections:

1. Introduction and background
2. Overview of the GDPR
3. Changes under the GDPR
4. Application of the GDPR

This training is expected to take 90 minutes to complete. It is recommended that you work through the training manual in the order presented.

Once you have worked through the training manual, you will be given a **short multiple choice question (MCQ) assessment** for you to complete to demonstrate your understanding of the GDPR.

After completing this training manual and associated MCQ assessment, it is recommended that you seek guidance from your employer, superintendent pharmacist or the person dealing with data protection within the pharmacy, to familiarise yourself with any additional policies and/or procedures which may be applicable to the pharmacy organisation.

© The National Pharmacy Association. March 2018. Produced by the NPA Pharmacy team.

Community Pharmacy GDPR Working Party

Aims to highlight a **united approach** to GDPR, identify the overall **impact** of GDPR and produce **sector specific guidance**

Guidance for Community Pharmacy (Part 1)

- Providing sector-specific information

Guidance for the Community Pharmacy (short version) (Part 2)

- Useful to help in training members of your team

Workbook for Community Pharmacy (Part 3)

- Templates for you to amend as appropriate for your pharmacy; such as for the recording all your pharmacy processes and a privacy notice

FAQs for Community Pharmacy (Part 4)

- For further information

The General Data Protection Regulation and associated legislation

Part 3: Workbook for Community Pharmacy

Version 1: 25th March 2018

Community Pharmacy
GDPR Working Party

Contents

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.

Revalidation

What is revalidation?

Revalidation:
*A mechanism for healthcare professionals to demonstrate their skills are **up-to-date** and that they remain **fit to practice***

New revalidation framework

- Four CPD records
- One record of peer discussion
- One reflective account

Who does it affect?

- **All** GPhC registered pharmacists and pharmacy technicians
- **Not** affected by individual factors, including:
  - Part-time employment
  - Non patient-facing roles
  - Living/working outside of the UK

Timeline – what lies ahead

- **30 March 2018**
  - Go live date for revalidation - recording of CPDs can begin on new online portal
  - CPDs on the old portal will become read-only - registrants can print off old CPD entries
- **1 June 2018**
  - Old portal goes offline - ensure you have downloaded previous CPD entries

Revalidation framework timeline

Example

If your registration expires on **31 December 2018**:

1. You are required to submit only **four** CPD entries as part of your renewal – can only be submitted once your renewal window opens on **1 September 2018 until 31 October 2018**
2. When your registration expires on **31 December 2019**, you will be required to submit **all six** records as part of your renewal which will **include one reflective account and one peer discussion**

CPD records

- Each year, pharmacists and pharmacy technicians must submit **four** CPD entries
  - At least **two** must be planned learning activities

Top tips for completing revalidation records: CPD

- ✓ Include a specific learning objective
- ✓ Make it clear how the learning is relevant to your role
- ✓ Explain how the learning will affect individuals using your services
- ✓ Describe learning activities
- ✓ Explain how the learning has been applied
- ✓ Provide examples of the benefits of the learning to service users
- ✓ Provide any feedback or evidence
- ✓ Include any next steps

Peer discussion

- Each year, pharmacy pharmacists and pharmacy technicians must submit **one** record of a peer discussion
- A **peer discussion** is *an activity undertaken through engagement with others, involving reflection on learning and practice*
- <u>However</u> a **peer review** is *a learning and development activity that encourages engagement and involves an assessment of performance*

Peer discussion

- Peer discussions should:
  - Be open and honest
  - Relate to activities from the past **year**
  - Help you reflect on your practice to help make improvements

Top tips for completing revalidation records: peer discussion

- ✓ Include a description of why this peer was chosen
- ✓ Explain how the peer discussion has helped you reflect on your practice
- ✓ Describe changes made to your practice as a result
- ✓ Provide examples of how the changes implemented have positively impacted and benefited your service users
- ✓ Be between 200- 400 words

Reflective account

- Each year, pharmacy professionals must submit **one** record of a reflective account

- A reflective account is *an activity designed to encourage pharmacy professionals to think about the way in which they work in relation to the GPhC standards*

Reflective account

- The reflective account should include:

A summary of you practice from the past year

How one of more of the GPhC standards for pharmacy professionals have been met

Examples of how individuals using your services have benefited

Top tips for completing revalidation records: reflective account

- ✓ Describe the setting of your practice and your main roles
- ✓ Include a description of the typical users of your service(s)
- ✓ Explain how you have met the GPhC standard(s) for pharmacy professionals
- ✓ Include examples
- ✓ Include any feedback or evidence

Review of records

- Minimum of **2.5%** of registrants selected for full review
- Reviewed against set criteria
  - Core
  - Feedback
- Undertaken by a pharmacy **professional and lay reviewer**
- Tailored feedback provided
- **No** feedback score

FAQs

How long will it take to complete the six records and when do these need to be submitted by?

- For CPD records, approximately 4.5 hours
- For the peer discussion (including arranging the discussion and the write up) 2 to 5 hours
  - The peer discussion itself is expected to be around 30 minutes to one hour
- For the reflective account, approximately an hour
- These records must be submitted each year, at the same time registration renewal is completed

If I miss the submission deadline or I cannot complete/submit all the records, will I be able to renew my registration?

- When renewing registration, registrants must declare that you will comply with the revalidation framework
- If unable to submit some/all records - inform GPhC in advance of renewal
- Dependant on individual circumstances/reasons, **may still be able to renew registration**
- Without good reasons, you will enter a remediation process

Who can be a peer and how do I find a peer?

- A number of examples:
  - Another pharmacy professional
  - Another health professional
  - A non-health professional that has an insight into your role
  - Someone you work with
  - A group of individuals in a similar role
- **Not** an individual with which you have a close relationship with (such as a family member or friend)

Falsified Medicines Directive (FMD)

FMD: background

Aims to prevent falsified medicines entering the supply chain

- **Two** mandatory safety features
  - an **anti-tamper device (ATD)** **and**
  - **unique identifier (UI)** in the form of a 2D barcode
- To be implemented from **9 February 2019**
  - The impact of Brexit is currently unknown

FMD medicine safety features

Anti-tampering device

Safety features

Unique Identifier

Verifying and authenticating medicines

Manufacturers enter each medicines UI code to the **National Medicines Verification System** (SecurMed UK)

Pharmacies will be required to authenticate medicines "*at the time of supplying it to the public*"

This includes checking the **ATD** is still intact

And **scanning the UI** on the medicines outer packaging – referred to as '**decommissioning**'

Verifying and authenticating medicines

- There are two potential messages displayed once the UI has been scanned:

"Active"

- Medicine can be dispensed as long as the ATD is undamaged
- If the ATD is broken in order to dispense the medicine, this is exempt
- Successfully **decommissioned**

"Inactive"

- **Cannot** be supplied
- Additional messages include "already dispensed", "recalled", "withdrawn", "stolen" or "locked"

Decommissioned medicines

- Decommissioned medicine status change from:

- If the product is not supplied, the status can be reversed

Reversing the medicine status

- Reversing the "***decommissioned***" status of a medicine can only occur if:
  - It takes place at the **same pharmacy** it was decommissioned
  - It occurs no more than **10 days** after decommissioning
  - The product has **not expired**
  - The product has not been recalled, withdrawn, stolen or intended for destruction

Implications for pharmacy contractors

- All community pharmacies will be required to:
  - Connect to the UK National Medicines Verification System
  - Update software
  - Obtain scanners
  - Introduce SOPs

Scanning and decommissioning medicines

*"**At the time of supplying it to the public**" is not defined but the FMD process must be completed before the medicine is released to the patient*

- **'Aggregated barcodes'** may can be used where more than one medicine is dispensed
  - This code links multiple items together and allows decommissioning of all items in one go by scanning the aggregated code on the bag label

Potential decommissioning points

During assembly

During accuracy check

At point of hand out

At point of hand out with aggregated code

Decommissioning points and patient safety concerns

During assembly

or

during accuracy check

- Additional step/increase workload
- Time period between assembly and handing out
- Increased pressure/distraction

Decommissioning points and patient safety concerns

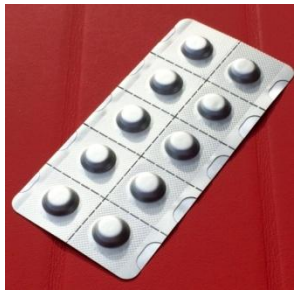
At point of hand out with/without aggregated code

- Prescription bags need to be re-opened
- Training required for all support staff
- Increased workload/pressure

FAQs

Do GSL and P medicines need to be decommissioned before supplying?

- Non-prescription medicines are **not** included under FMD
- Therefore do **not** require decommissioning
  - The only exception is OTC omeprazole
- Unlicensed specials and appliances/devices do **not** require decommissioning



How do I deal with medicines that do not have a UI code?

- There may be medicines in the supply chain which do not have a 2D barcode by **February 2019**
- These can still be dispensed
- They are **not** required to be decommissioned

Who will pay for the additional equipment and training required?

- Pharmacies will be responsible for any costs associated with obtaining or updating software and hardware
- Total costs unknown

Interim quality payments scheme

Interim funding arrangements 2018/19

- Announced in March 2018
- **No** changes to the following:
  - Fees and allowances from April 2018
  - Funding levels — remain at the 2017/18 level
  - Single Activity Fee (SAF) —remains at £1.29
  - Establishments Payments
  - Pharmacy Access Scheme (PhAS) payments — pharmacies already receiving PhAS payments will continue to receive them on a monthly basis

Interim quality payments (QP) scheme 2018/19

- Further £37.5 million invested
- One review point on **29 June 2018**
- Payments claim window
  - 9am Monday 11 June 2018 to 11.59pm Friday 13 July 2018
- Remains largely the same as 2017/18, with a few amendments
- Each point worth a minimum £32 and maximum £64 (no reconciliation payment)

Interim QP scheme – gateway criteria

- **Two** changes to the gateway criteria:

1 - NHS Choices – Bank Holiday (BH) opening hours

- Now required to include BH opening hours for 2018/19 on NHS Choices profile
- Create a '*Public holiday and other special day*' entry – refer to NHS Choices user guide
- Failure to add BH opening hours to NHS Choices profile → gateway criteria will **not be** met
- BH hours to be used by local NHS England teams to plan service provision

Interim QP scheme – gateway criteria

NHS Choices - Distance selling pharmacy (DSP) only:

- No longer required to complete a survey as requested for the November 2017 review point
- DSP contractors are instead requested to follow the process outlined in the NHS England guidance – to be published shortly

Interim QP scheme – gateway criteria

2 - NHS mail – shared account

- Send and receive NHSmail from the pharmacy premises **shared NHSmail account**
- **Relevant** members of pharmacy team must have own personal NHSmail address linked to the pharmacy's shared NHSmail mailbox
- Using personal NHSmail accounts to send and receive NHSmail, instead of a pharmacy premises shared NHSmail account, will not meet the gateway criterion

Interim QP scheme – quality criteria

- **No changes** to quality criteria
- Number of quality points per criterion same as total number of points across **both** review points in 2017/18 – 100 points in total

Important points to note

- **Patient safety report**
  - If claimed in 2017, new report required
  - Review and update previous report since submission in 2017

Interim QP scheme – quality criteria

Important points to note

- **Patient survey**
  - If claimed in 2017, cannot reuse same results report
  - Undertake new survey, produce new report and publish on NHS Choices profile
- **Summary Care Records (SCR)**
  - New time periods to compare SCR access
  - Period 1 – 1 May 2017 to 26 November 2017
  - Period 2 – 4 December 2017 to Sunday 1 July 2018

Interim QP scheme – quality criteria

Important points to note

- **NHS 111 Directory of Services (DoS)**
  - Edit/confirm accuracy of information on pharmacy's DoS profile on **new DoS Profile Updater – available soon**
  - Complete by **11.59pm on 29 June 2018**
- **Asthma review**
  - If claimed in 2017, a new review of patients since 24 November 2017

Questions?

Thank you!

NPA Pharmacy team: 01727 891 800
or
NPA Chief Pharmacist, Leyla Hannbeck at
L.hannbeck@npa.co.uk