Community Pharmacy England

NHS England

2026 Data Security and Protection Toolkit Toolkit Workshop

Wednesday 11th February 2026
7.30-8.30pm

Community Pharmacy England

Data Security and Protection Toolkit Workshop: Introduction

John Hodson

NHS DSPTK team

Katrina Worthington

Regulations Officer

Daniel Ah-Thion

Community Pharmacy IT Policy Manager

Community Pharmacy England

NHS England

In this webinar

- Toolkit submission this year
- Changes with this version
- Pharmacy guidance & templates
- Q&A

Get involved: ask us questions via Slido tool

Please submit your questions through Slido

Go to www.slido.com and enter code #2785604.

Or simply scan this QR code.

You may find it helpful to use a separate device e.g. smartphone.

Key messages

Pharmacy toolkit launched

The Pharmacy Toolkit has been launched and can now be completed by pharmacy teams. The deadline for completion is June 30th.

Pharmacy-specific Info

The 'tool tips' included in the Toolkit contain pharmacy-specific information to guide teams through the process.

GDPR Workbook

The Community Pharmacy England GDPR workbook can be completed to confirm 'see GDPR WB' for many questions in the Toolkit.

Guidance available

Community Pharmacy England has provided guidance on the Toolkit at cpe.org.uk/ds.

Publicly shared status

The DSPTK status of pharmacies is available publicly and shared with NHS England.

Supplier support

Suppliers can help pharmacy IG leads that are completing their DSPTK.

Community Pharmacy England NHS England

What is the Data Security and Protection Toolkit

Annual online self-assessment

NHS organisations must complete this data security self-assessment by June 30th each year to measure compliance with the NDG Data Security Standards

Measure against NDG standards

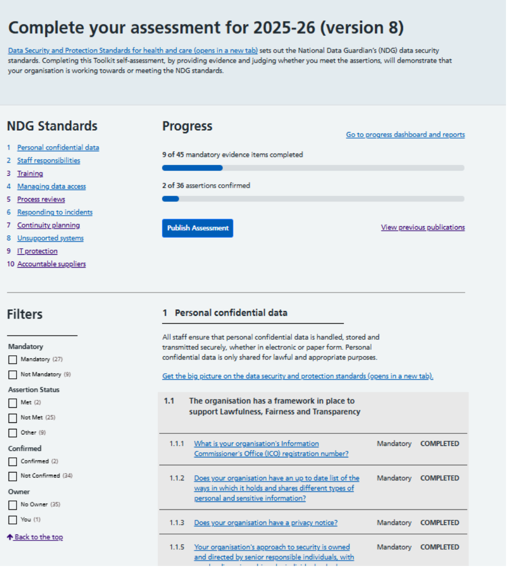
The Toolkit enables NHS organisations to assess their data security and protection practices against the 10 NDG Data Security Standards

Comply with GDPR & cyber hygiene

Completing the Toolkit helps organisations comply with GDPR requirements and maintain basic cyber security hygiene

Mandatory for NHS organisations

All NHS organisations are required to complete the Toolkit annually



Complete your assessment for 2025-26 (version 8)

Data Security and Protection Standards for health and care (opens in a new tab) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

NDG Standards

1 Personal confidential data
2 Staff responsibilities
3 Training
4 Managing data access
5 Process reviews
6 Responding to incidents
7 Continuity planning
8 Unsupported systems
9 IT protection
10 Accountable suppliers

Progress

Go to progress dashboard and reports

9 of 45 mandatory evidence items completed

2 of 36 assertions confirmed

Filters

Mandatory
□ Mandatory (27)
□ Not Mandatory (9)

Assertion Status
□ Met (2)
□ Not Met (25)
□ Other (9)

Confirmed
□ Confirmed (2)
□ Not Confirmed (34)

Owner
□ No Owner (35)
□ You (1)

1 Personal confidential data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

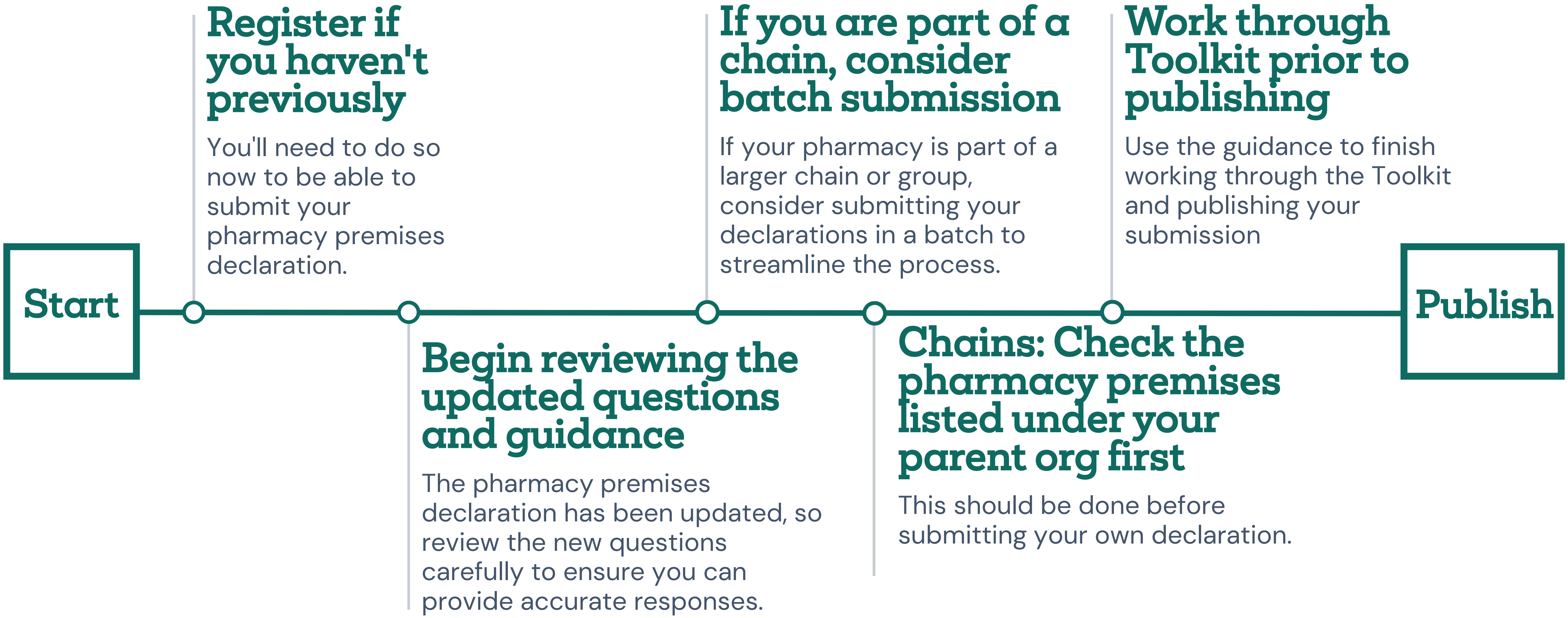
Get the big picture on the data security and protection standards (opens in a new tab).

1.1	The organisation has a framework in place to support Lawfulness, Fairness and Transparency		
1.1.1	What is your organisation's Information Commissioner's Office (ICO) registration number?	Mandatory	COMPLETED
1.1.2	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	Mandatory	COMPLETED
1.1.3	Does your organisation have a privacy notice?	Mandatory	COMPLETED
1.1.5	Your organisation's approach to security is owned and directed by senior responsible individuals, with	Mandatory	COMPLETED

Community Pharmacy England

NHS England

What you need to do (summary)



Start

Register if you haven't previously

You'll need to do so now to be able to submit your pharmacy premises declaration.

Begin reviewing the updated questions and guidance

The pharmacy premises declaration has been updated, so review the new questions carefully to ensure you can provide accurate responses.

If you are part of a chain, consider batch submission

If your pharmacy is part of a larger chain or group, consider submitting your declarations in a batch to streamline the process.

Chains: Check the pharmacy premises listed under your parent org first

This should be done before submitting your own declaration.

Work through Toolkit prior to publishing

Use the guidance to finish working through the Toolkit and publishing your submission

Publish

Overview of guidance

Guidance materials

Overview DSPTK briefing: Five steps for completing the Toolkit.

Data security webpages

Question-by-question support

PDF

Spreadsheet

These cover each Toolkit question

Additional NHS support

FAQs

Training Tool

Exeter Helpdesk

Toolkit training events

Logging in to the Toolkit

Access the Toolkit

Go to the DSPT Toolkit website at dsptoolkit.nhs.uk

Click the 'Log in' button

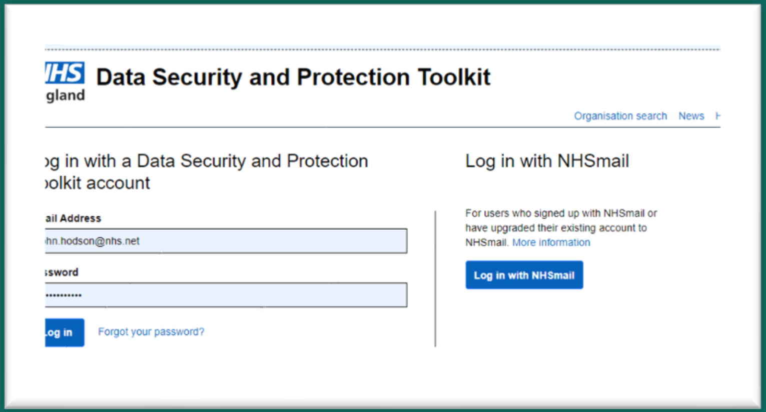
Look for the 'Log in' option in the top right corner of the page

Use your login credentials

Enter the login details you used last year to access the toolkit

Reset your password if needed

Use the 'Forgot your password?' option to reset your password if you can't remember it



Data Security and Protection Toolkit

og in with a Data Security and Protection olkit account

ail Address: hn.hodson@nhs.net

ssword: ••••••••••

Log in with NHSmail

For users who signed up with NHSmail or have upgraded their existing account to NHSmail. More information

Completing your Organisation Profile (1)

Log in and navigate to the Organisation Profile

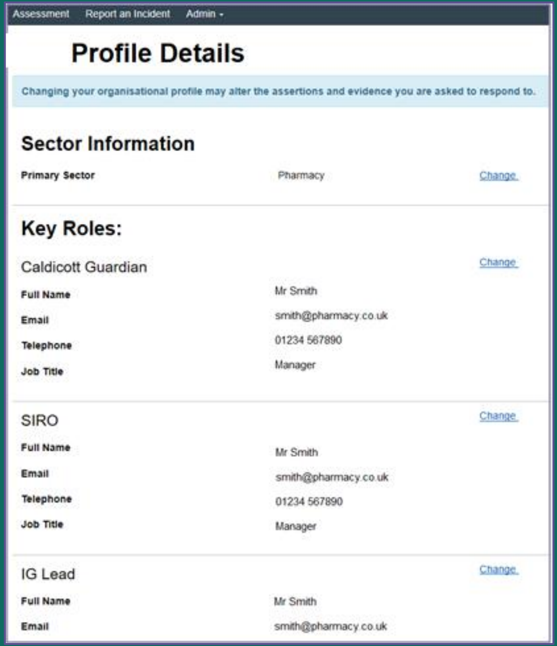
After logging in, click on the 'Admin' menu and then select 'Organisation Profile' to access the organisation's profile information.

Enter key roles

In the Organisation Profile, enter the key roles for the pharmacy, including the Caldicott Guardian, SIRO (Senior Information Risk Owner), and IG Lead (Information Governance Lead).

Update your contact information

Review your contact information.



Profile Details

Changing your organisational profile may alter the assertions and evidence you are asked to respond to.

Sector Information

Primary Sector	Pharmacy	Change

Key Roles:

Caldicott Guardian — Change

Full Name	Mr Smith
Email	smith@pharmacy.co.uk
Telephone	01234 567890
Job Title	Manager

SIRO — Change

Full Name	Mr Smith
Email	smith@pharmacy.co.uk
Telephone	01234 567890
Job Title	Manager

IG Lead — Change

Full Name	Mr Smith
Email	smith@pharmacy.co.uk

Completing your Organisation Profile (2)

NHSmail is the only email system approved for securely sharing patient data. Both the sender and receiver must have NHSmail accounts for full encryption.

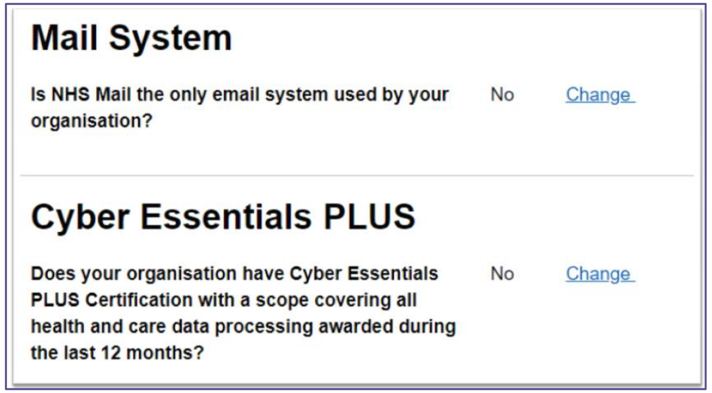
Cyber Essentials PLUS certification is unlikely to apply to most pharmacies due to the limited scope of the program.

Confirm NHSmail use

Avoid sharing NHSmail logins

Cyber Essentials PLUS

NHSmail login details must not be shared among staff to maintain security and accountability.



Mail System

Is NHS Mail the only email system used by your organisation?	No	Change

Cyber Essentials PLUS

Does your organisation have Cyber Essentials PLUS Certification with a scope covering all health and care data processing awarded during the last 12 months?	No	Change

Refreshing the GDPR Workbook

Refresh GDPR Workbook

Ensure the GDPR workbook is up-to-date and compliant with the latest regulations

Paste 'See GDPR WB'

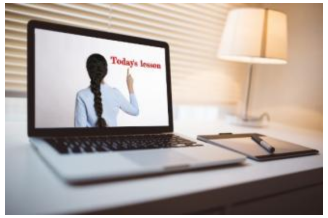
Insert the phrase 'See GDPR WB' into approximately half of the questions to provide the necessary context, where these have been actioned

Organization profile update

The 'GDPR WB completed' option is **no longer** available within the organization profile

Regularly refreshing the GDPR workbook and updating the organization profile ensures your pharmacy remains compliant with data protection regulations.

Staff training considerations



Mandatory training requirement

95%+ of staff must complete training each year to mitigate risks and protect data

Data security training

Pharmacy data security and IG training or GDPR staff training booklet from Community Pharmacy England meets this requirement

Training log maintenance

The training log could be re-dated to confirm all staff have gone through it again

DSPTK pharmacy policies

When organisations put IG rules and procedures in place, staff members (including employees, locums, students, etc) need to follow them. This will ensure that everyone, including patients, can be more confident that information is:

- properly protected;
- only shared when it is right and proper to do so;
- accurate and up to date; and
- available when and where it is needed.

Ultimately, it means that your pharmacy will be able to deliver the best possible service to your patients, with reduced risk of reputation damage (or the need to pay a fine) for breach of confidentiality.

Why is data security and IG important?

IG rules and procedures enable us to make sure that we provide a confidential service and that patients can continue to trust us to look after their information.

A Confidential Service: Patient information is confidential. There can be no truly confidential service unless everyone who works in or with the NHS knows what information is 'confidential' and how to keep it confidential. We all need to make sure information is kept secure and report incidents if it goes wrong. How else will we learn and get better?

Every one of us must contribute. No matter how often or how rarely you have contact with patients or information about patients you should report any problems that you see. If problems aren't recognised, they will not be reported and are in danger of becoming accepted working practice.

A confidential service means all organisations and employees providing care or treatment to patients have a duty of confidentiality – not just the members of the pharmacy staff that patients have direct contact with.

Patient Trust: Patients trust the NHS and your pharmacy, to record information about their health, look after the information securely and only give it to those who need to see it.

"*Patient Information Held Securely!*" is not a headline you will see in a national newspaper because patients expect (and it is enforced by law) that their information will be properly looked after. Everyone providing services to patients is in a position of public trust – and everyone has to work hard to avoid failures that not only could cause significant patient embarrassment or distress but could become the next day's headline and lead to fines against the pharmacy or staff.

To keep patient information confidential, secure, accurate and up to date - **everyone** must help.

Headline News!

[illegible]

Page 2 of 18

Ongoing staff training is critical for maintaining data security and mitigating operational risks within the organization.

Overview of the Batch Submission feature

Who is this feature for?

This feature is for use by pharmacy organisations with **three or more** pharmacies.

Uses NHS Parent Organisation Code (POC)

The feature uses the NHS Parent Organisation Code (POC) to associate pharmacy premises with the correct organisation.

Importance of accurate POC linking

It is critical that pharmacy premises are associated with the right POC, particularly after any ownership change, as it impacts data and other issues.

Adjusting POC associations

The POC association can be adjusted as required, and guidance is available at cpe.org.uk/POC.

Additional how-to batch submission guidance

CPE also have specific guidance and a batch submission how-to guide to assist with checking your pharmacies linked to your POC cpe.org.uk/tk.

Community Pharmacy England

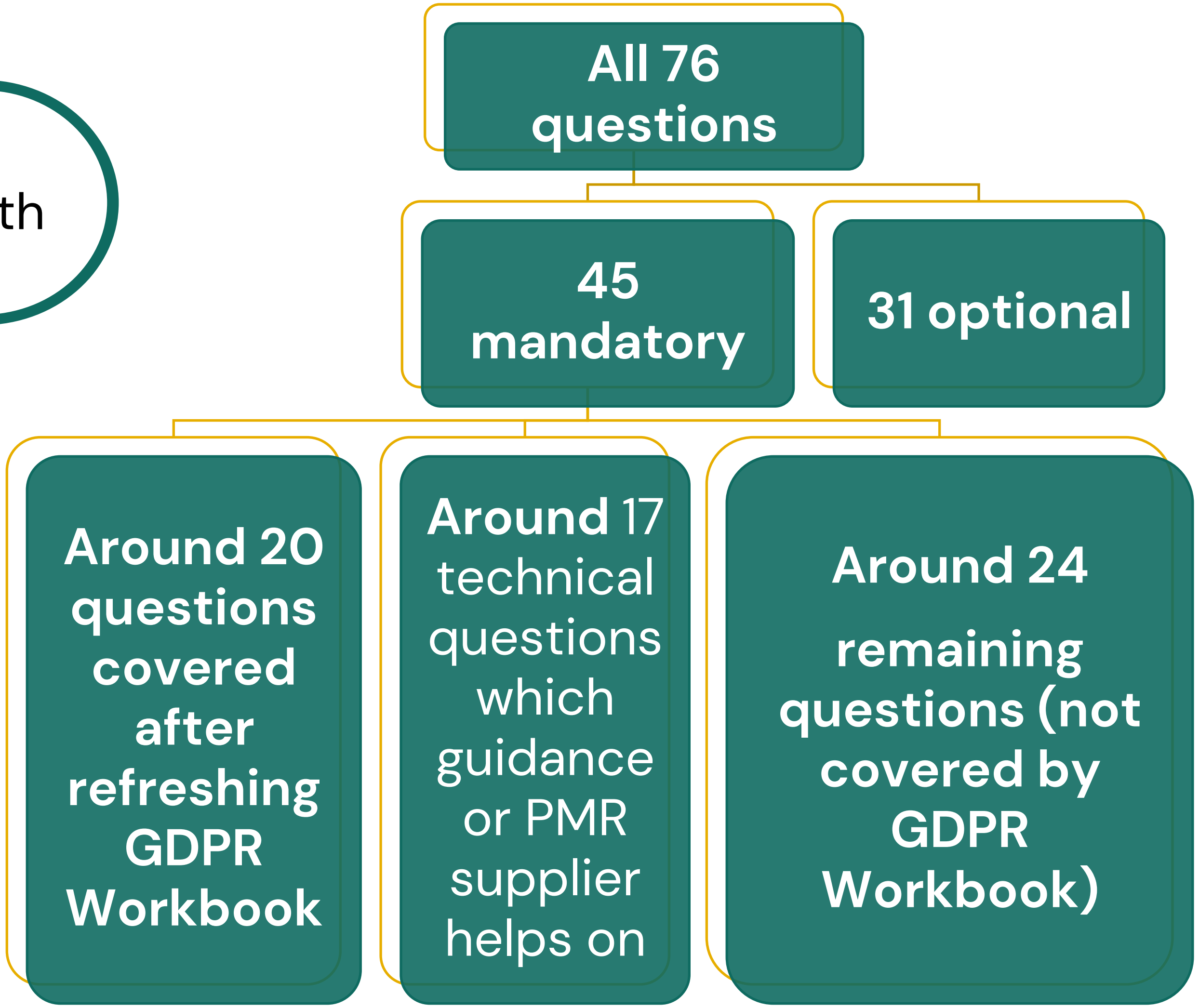
NHS England

Types of questions

NHS DSPTK team, Community Pharmacy England, and IT suppliers have supported reducing pharmacy workload involved with completion but supporting standards

Around half of questions can be marked ‘see GDPR WB’ if you have refreshed the GDPR WB

IT suppliers may help answer technical questions



All 76 questions

45 mandatory

31 optional

Around 20 questions covered after refreshing GDPR Workbook

Around 17 technical questions which guidance or PMR supplier helps on

Around 24

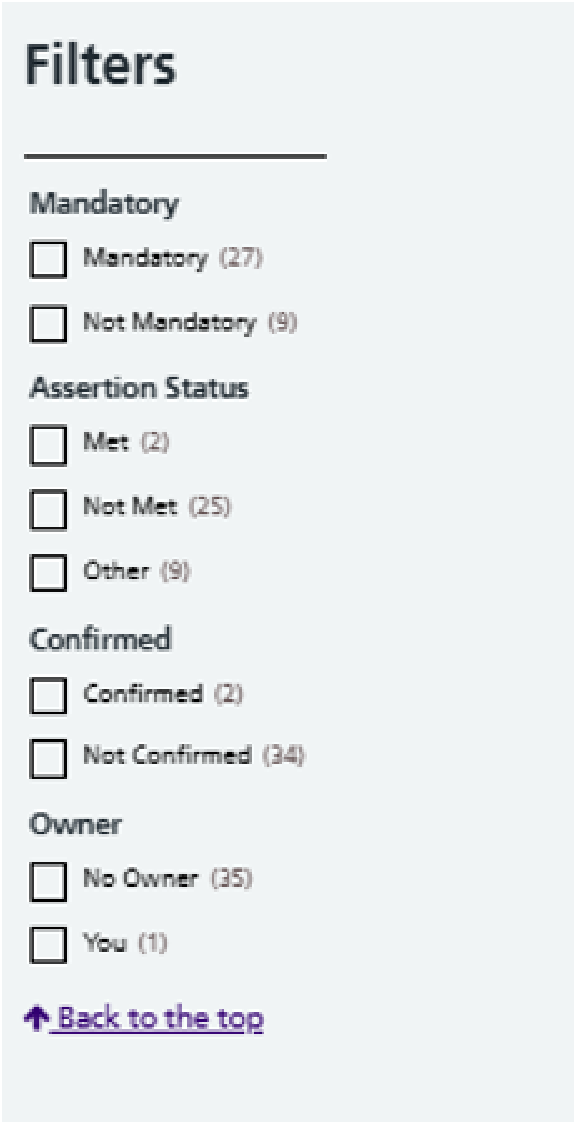
remaining questions (not covered by GDPR Workbook)

Completing the mandatory questions

Mandatory questions have the word ‘mandatory’ by their side

The ‘optional’ questions do not require completion

Tick: Items have been unticked this year, you need to ensure you are happy to confirm them.



Filters

Mandatory

□ Mandatory (27)

□ Not Mandatory (9)

Assertion Status

□ Met (2)

□ Not Met (25)

□ Other (9)

Confirmed

□ Confirmed (2)

□ Not Confirmed (34)

Owner

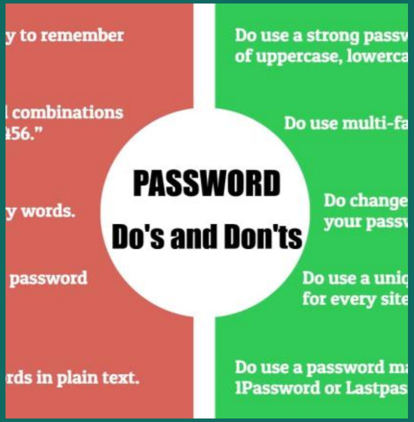
□ No Owner (35)

□ You (1)

↑ Back to the top

Toolkit question 4.3.1 :

System Administrators



- The people within your organisation who are IT system administrators may have access to more information than other staff. Therefore, they need to be held accountable in a formal way to higher standards of confidentiality than others.

- There is a community pharmacy system administrator template (cpe.org.uk/dstemplates)

This questions has been upgraded due to cyber incidents impacting system administrators have a much greater impact than standard users

Toolkit question 4.5.3: Multi-Factor Authentication

Mandatory Question

The toolkit now includes a mandatory question about multi-factor authentication.

Multi-Factor Authentication

Multi-factor authentication (MFA) is a security process that requires more than one method of authentication to verify a user's identity.

Purpose of MFA

MFA adds an extra layer of security to protect against unauthorized access, even if a password is compromised.

Common MFA Methods

Common MFA methods include SMS/email codes, biometrics (fingerprint, face ID), and hardware security keys.

The mandatory question on multi-factor authentication in the toolkit emphasizes the importance of implementing strong security measures to protect against unauthorized access.

MFA headlines

Why add MFA to DSPT?

- Global consensus that MFA is *"one of the most effective ways to protect … against unauthorised access,"* even the crudest forms of MFA providing robust defence against commodity attacks.
- Our threat model is *"opportunistic attacks by capable and motivated profit-seeking actors…"* against which MFA provides strong defence and deterrent.

Why MFA is important?

- **Policy objective** is for a rapid widespread increase in MFA usage as a fundamental cyber security control that is extremely effective against the typical attacks seen in the NHS. It is not intended to require 'best of breed' solutions, or complex identity management systems.
- **Signal to market** that MFA is a must for digital offerings for pharmacy.

Future

- **Will strengthen over time:** DSPTK and IT supplier MFA elements will strengthen

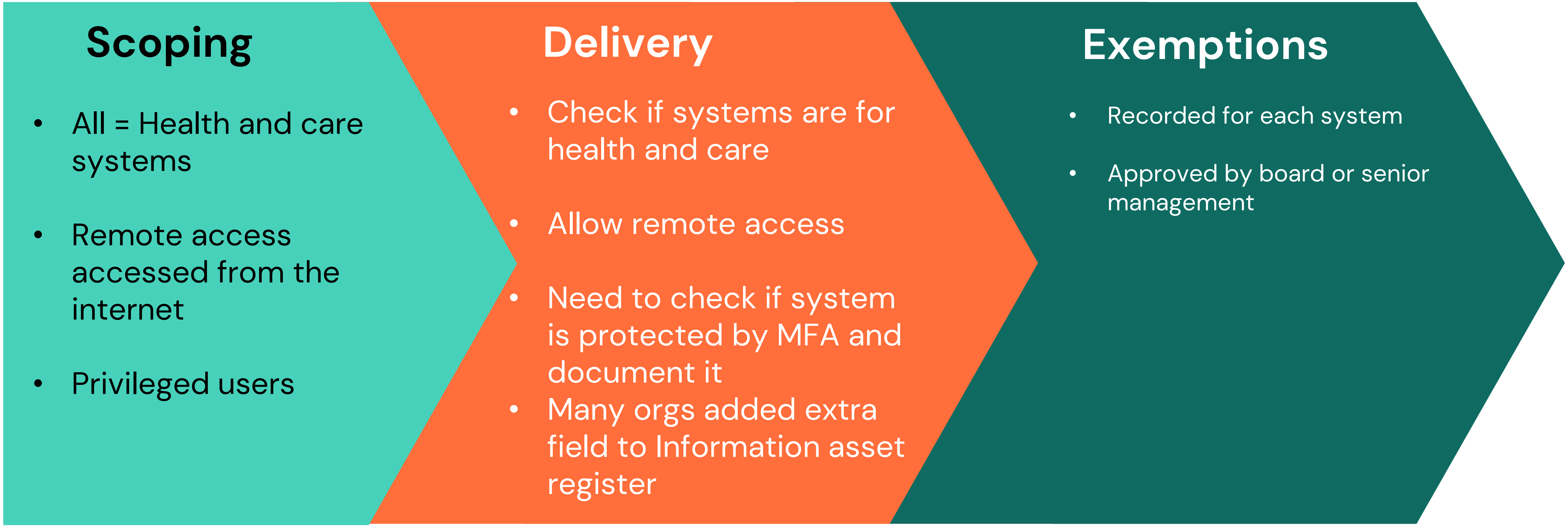
Toolkit question 7.1.1 change Digital Asset Register

- Have you got a a list of the digital devices (hardware) and computer software your organisation uses.
- Has it been reviewed at least once in the last twelve months.
- There is a community pharmacy assett register template (cpe.org.uk/dstemplates / cpe.org.uk/dstraining)

- The question will invite you to upload your document or refer to where you store your asset document

Understanding your assets is vital to making them secure

How to answer the MFA question



Scoping

- All = Health and care systems
- Remote access accessed from the internet
- Privileged users

Delivery

- Check if systems are for health and care
- Allow remote access
- Need to check if system is protected by MFA and document it
- Many orgs added extra field to Information asset register

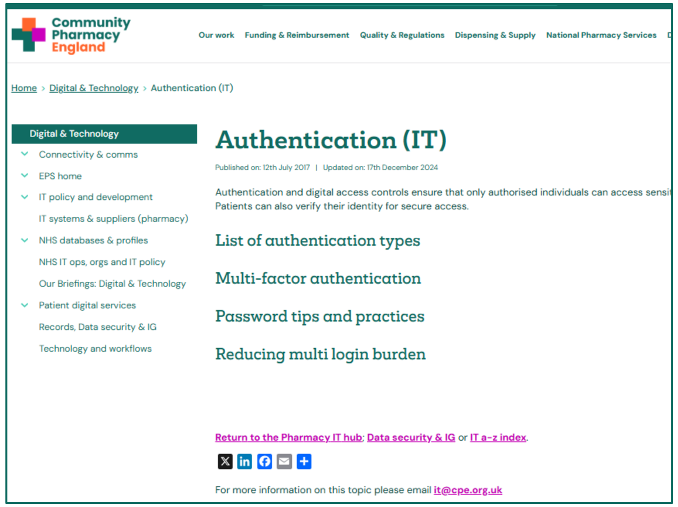
Exemptions

- Recorded for each system
- Approved by board or senior management

MFA support: Community Pharmacy England & NHS England

Get MFA guidance from Community Pharmacy England

The Community Pharmacy England (CPE) website provides comprehensive guidance on implementing and using multi-factor authentication (MFA) for community pharmacies.



Home › Digital & Technology › Authentication (IT)

Digital & Technology
- Connectivity & comms
- EPS home
- IT policy and development
- IT systems & suppliers (pharmacy)
- NHS databases & profiles
- NHS IT ops, orgs and IT policy
- Our Briefings: Digital & Technology
- Patient digital services
- Records, Data security & IG
- Technology and workflows

Authentication (IT)

Published on: 12th July 2017 | Updated on: 17th December 2024

Authentication and digital access controls ensure that only authorised individuals can access sensi
Patients can also verify their identity for secure access.

List of authentication types

Multi-factor authentication

Password tips and practices

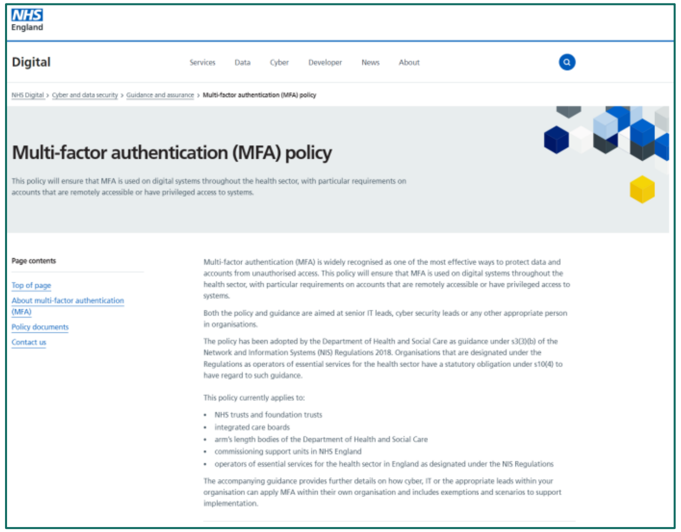
Reducing multi login burden

Return to the Pharmacy IT hub; Data security & IG or IT a-z index.

For more information on this topic please email it@cpe.org.uk

Consider NHS England's MFA policy

The NHS England MFA policy outlines the requirements and best practices for implementing MFA across the healthcare system.



NHS Digital › Cyber and data security › Guidance and assurance › Multi-factor authentication (MFA) policy

Multi-factor authentication (MFA) policy

This policy will ensure that MFA is used on digital systems throughout the health sector, with particular requirements on accounts that are remotely accessible or have privileged access to systems.

Page contents

- Top of page
- About multi-factor authentication (MFA)
- Policy documents
- Contact us

Multi-factor authentication (MFA) is widely recognised as one of the most effective ways to protect data and accounts from unauthorised access. This policy will ensure that MFA is used on digital systems throughout the health sector, with particular requirements on accounts that are remotely accessible or have privileged access to systems.

Both the policy and guidance are aimed at senior IT leads, cyber security leads or any other appropriate person in organisations.

The policy has been adopted by the Department of Health and Social Care as guidance under s3(3)(b) of the Network and Information Systems (NIS) Regulations 2018. Organisations that are designated under the Regulations as operators of essential services for the health sector have a statutory obligation under s10(4) to have regard to such guidance.

This policy currently applies to:

- NHS trusts and foundation trusts
- integrated care boards
- arm's length bodies of the Department of Health and Social Care
- commissioning support units in NHS England
- operators of essential services for the health sector in England as designated under the NIS Regulations

The accompanying guidance provides further details on how cyber, IT or the appropriate leads within your organisation can apply MFA within their own organisation and includes exemptions and scenarios to support implementation.

Community Pharmacy England

NHS England

IT supplier support (including MFA)

Supplier documentation and help materials

IT suppliers may provide pharmacies with documentation and help materials to assist with implementing and using their systems

MFA and other data security resources

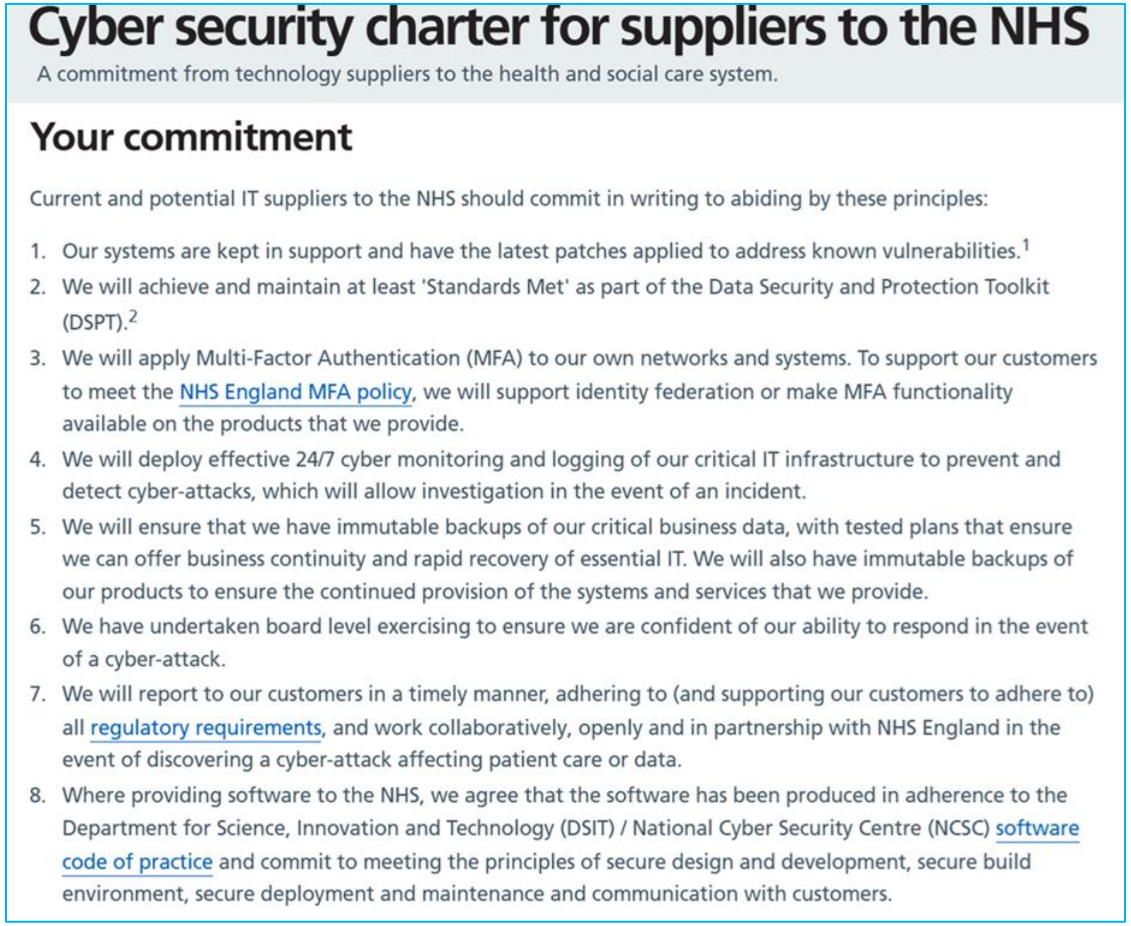
Some IT suppliers offer security-related resources on their website or via email to help pharmacies with their security toolkit

Pharmacist support

IT suppliers can provide direct support and guidance to pharmacy teams to help them effectively utilize the supplier's systems and tools

IT suppliers can be a valuable resource for pharmacies, providing a range of materials and support to help teams implement and use their products effectively.

Cyber Security charter for IT suppliers to the NHS



Cyber security charter for suppliers to the NHS

A commitment from technology suppliers to the health and social care system.

Your commitment

Current and potential IT suppliers to the NHS should commit in writing to abiding by these principles:

1. Our systems are kept in support and have the latest patches applied to address known vulnerabilities.[1]
2. We will achieve and maintain at least 'Standards Met' as part of the Data Security and Protection Toolkit (DSPT).[2]
3. We will apply Multi-Factor Authentication (MFA) to our own networks and systems. To support our customers to meet the NHS England MFA policy, we will support identity federation or make MFA functionality available on the products that we provide.
4. We will deploy effective 24/7 cyber monitoring and logging of our critical IT infrastructure to prevent and detect cyber-attacks, which will allow investigation in the event of an incident.
5. We will ensure that we have immutable backups of our critical business data, with tested plans that ensure we can offer business continuity and rapid recovery of essential IT. We will also have immutable backups of our products to ensure the continued provision of the systems and services that we provide.
6. We have undertaken board level exercising to ensure we are confident of our ability to respond in the event of a cyber-attack.
7. We will report to our customers in a timely manner, adhering to (and supporting our customers to adhere to) all regulatory requirements, and work collaboratively, openly and in partnership with NHS England in the event of discovering a cyber-attack affecting patient care or data.
8. Where providing software to the NHS, we agree that the software has been produced in adherence to the Department for Science, Innovation and Technology (DSIT) / National Cyber Security Centre (NCSC) software code of practice and commit to meeting the principles of secure design and development, secure build environment, secure deployment and maintenance and communication with customers.

Cyber charter: Launch

NHS England has launched NHS cyber security supply chain charter.

IT supplier sign-up

IT suppliers are encouraged to begin signing-up now

A resilient NHS IT environment

This is a significant step towards enhancing the resilience and security of healthcare services and demonstrates dedication to being a trusted and secure partner to the health and care system.

Information from IT suppliers about… (1)

Evidence item	Text
1.4.2	If your organisation uses third parties to destroy records or equipment that hold personal data, is there a written contract in place that has been reviewed in the last twelve months? This contract should meet the requirements set out in data protection regulations.
1.4.3	If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?
4.2.4	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?
4.5.3	Multi-factor authentication is used on all remotely accessible user accounts on all systems, with exceptions only as approved by your board or equivalent senior management.
6.2.1	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?
7.3.1	How does your organisation make sure that there are working backups of all important data and information?
7.3.4	Are backups routinely tested to make sure that data and information can be restored?

Information from IT suppliers about... (2)

Evidence item number	Text
8.1.4	Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?
9.1.1	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?
9.5.2	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?
10.1.2	Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?
10.2.1	Do your organisation’s IT system suppliers have cyber security certification?

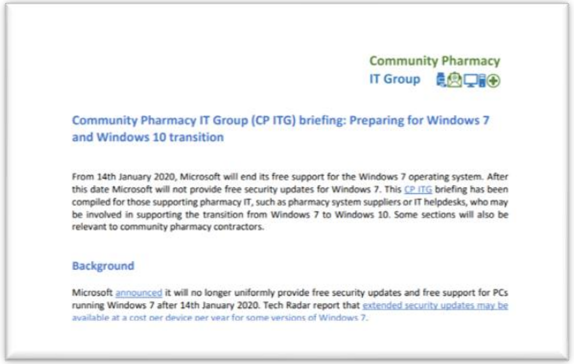
Toolkit questions 8.1.4 and 8.2.1: IT updates

Pharmacy IT updates

Ensure your pharmacy's software and systems are up-to-date to comply with the latest regulations and security requirements.

Windows transitions

Review the guidance on cpe.org.uk/windows for a smooth transition to the new Windows operating systems in your pharmacy.



Community Pharmacy
IT Group

Community Pharmacy IT Group (CP ITG) briefing: Preparing for Windows 7 and Windows 10 transition

From 14th January 2020, Microsoft will end its free support for the Windows 7 operating system. After this date Microsoft will not provide free security updates for Windows 7. This CP ITG briefing has been compiled for those supporting pharmacy IT, such as pharmacy system suppliers or IT helpdesks, who may be involved in supporting the transition from Windows 7 to Windows 10. Some sections will also be relevant to community pharmacy contractors.

Background

Microsoft announced it will no longer uniformly provide free security updates and free support for PCs running Windows 7 after 14th January 2020. Tech Radar report that extended security updates may be available at a cost per device per year for some versions of Windows 7.

Question 1.2.4: Opt-out system

Data flows	Pharmacy data flows reported
Data shared with <u>only</u> planning /research as reason Research: improving treatments Planning: improving services	✗
Data shared for an individual's care & treatment Between the pharmacy and a GP practice	✓
Legal requirement / public interest / consent There pharmacy legal requirement to dispense prescriptions	✓
Data is anonymised The data shared is anonymised	✓

Read more at cpe.org.uk/opt-out and within our question-by-question guidance

Community Pharmacy England

NHS England

Newer data uses: NHS GP Connect (NHS Direct Care APIs)

Pharmacy First Service

Pharmacy systems have begun to access records held by the GP and update the record held by the GP.

GP Connect use

GP Connect usage confirmed within MYS (Manage Your Service).

IT supplier privacy notice updates

Suppliers may update privacy notice if required to align with the arrangement.

Pharmacy privacy notice templates

Privacy notice and templates cover use of record information and passing information to other healthcare organizations (e.g., GP practices).

Additional services

Potentially additional services over time will involve pharmacy systems accessing and updating GP records.

Using the question-by-question guidance

Refer to question-by-question guidance

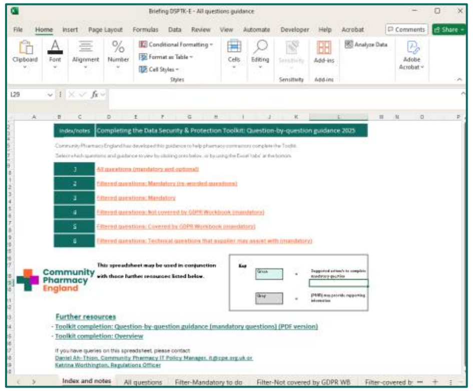
The pdf version or the spreadsheet version which can be filtered to display only those questions which are new or have been revised.

Summarises action and sets out how to do it

The guidance explains the summary actions to take for each Toolkit question.

Access additional templates and info

The guidance provides additional templates and information against each Toolkit question.



Index/notes	Completing the Data Security & Protection Toolkit: Question-by-question guidance 2025

Community Pharmacy England has developed this guidance to help pharmacy contractors complete the Toolkit.

Select which questions and guidance to view by clicking onto below, or by using the Excel 'tabs' at the bottom.

1	All questions (mandatory and optional)
2	Filtered questions: Mandatory (re-worded questions)
3	Filtered questions: Mandatory
4	Filtered questions: Not covered by GDPR Workbook (mandatory)
5	Filtered questions: Covered by GDPR Workbook (mandatory)
6	Filtered questions: Technical questions that supplier may assist with (mandatory)

This spreadsheet may be used in conjunction with those further resources listed below.

Key

Green	=	Suggested action/s to complete mandatory question
Grey	=	[PMR] may provide supporting information

Further resources

- Toolkit completion: Question-by-question guidance (mandatory questions) (PDF version)
- Toolkit completion: Overview

If you have queries on this spreadsheet, please contact
Daniel Ah-Thion, Community Pharmacy IT Policy Manager, it@cpe.org.uk or
Katrina Worthington, Regulations Officer

Briefing: Question-by-question guidance on how to complete the Data Security and Protection Toolkit (mandatory questions)

This document provides guidance for community pharmacy owners on how to complete the mandatory questions in the Data Security and Protection Toolkit (referred to as the 'Toolkit').

Pharmacy owners are required to answer all the mandatory questions in the Toolkit to make their annual information governance (IG) declaration.

Pharmacy teams that have already completed their General Data Protection Regulation (GDPR) Workbook ('GDPR WB'), which was previously released, should enter "See GDPR WB" for approximately half of the Toolkit questions. It's important to note that the GDPR WB is not available in the Toolkit.

Community Pharmacy England has also published this guidance in spreadsheet format. You can download the spreadsheet version of this guidance here: Question-by-question guidance (all questions) spreadsheet version.

Background and overview

To get started with completing the Toolkit, read the Briefing: Toolkit overview. This document provides instructions on how to:

- Login to the Toolkit;
- Begin updating and completing your "Organisation Profile";
- Ensure that your GDPR WB (General Data Protection Regulation Workbook) has been refreshed and marked as 'completed' within the organisation profile. This includes refreshing the personnel sections and contract sections-;
- Provide refresher training to your staff; and
- Use the "batch" submission feature, if applicable. Pharmacy owners with three or more pharmacies may find this feature beneficial. You can refer to the guide to learn how to use this feature and request its setup for your pharmacies.

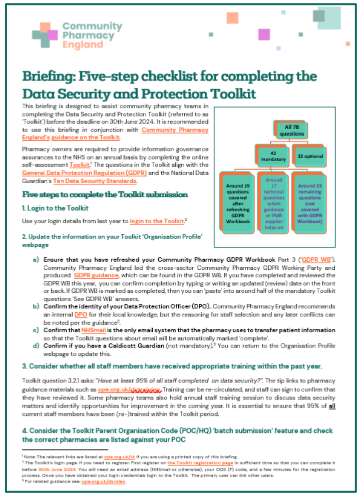
Please proceed to work through the outstanding Toolkit questions using the tables provided below. In the tables:

- Rows with a grey background signify technical questions that your IT support may be able to assist with (see final page).

Community Pharmacy England has collaborated with the DSPTK team to make the process of completing the Toolkit more manageable whilst maintaining data security. Key improvements in this year's Toolkit include:

- Enhancement to the Toolkit's layout;
- Improvements to the question wording and pharmacy-specific tips; and
- The Toolkit now displays the answers submitted by the pharmacy in the previous submission for various questions. This allows pharmacy teams to verify the accuracy of the information or adjust if necessary.

Table 1 of 2 includes those questions that are not covered if you have refreshed your GDPR WB.



Briefing: Five-step checklist for completing the Data Security and Protection Toolkit

This briefing is designed to assist community pharmacy teams in completing the Data Security and Protection Toolkit (referred to as 'Toolkit') before the deadline on 30th June 2024. It is recommended to use this briefing in conjunction with Community Pharmacy England's guidance on the Toolkit.

Pharmacy owners are required to provide information governance assurances to the NHS on an annual basis by completing the online self-assessment Toolkit.[1] The questions in the Toolkit align with the General Data Protection Regulation (GDPR) and the National Data Guardian's Ten Data Security Standards.

All 78 questions
42 mandatory
35 optional
Around 19 questions covered after refreshing GDPR Workbook
Around 17 technical questions which guidance or PMR supplier helps on
Around 23 remaining questions (not covered with GDPR Workbook)

Five steps to complete the Toolkit submission

1. Login to the Toolkit

Use your login details from last year to login to the Toolkit.[2]

2. Update the information on your Toolkit 'Organisation Profile' webpage

a) **Ensure that you have refreshed your Community Pharmacy GDPR Workbook** Part 3 ('GDPR WB'). Community Pharmacy England led the cross-sector Community Pharmacy GDPR Working Party and produced GDPR guidance, which can be found in the GDPR WB. If you have completed and reviewed the GDPR WB this year, you can confirm completion by typing or writing an updated (review) date on the front or back. If GDPR WB is marked as completed, then you can 'paste' into around half of the mandatory Toolkit questions 'See GDPR WB' answers.

b) **Confirm the identity of your Data Protection Officer (DPO).**. Community Pharmacy England recommends an internal DPO for their local knowledge, but the reasoning for staff selection and any later conflicts can be noted per the guidance[3].

c) **Confirm that NHSmail is the only email system that the pharmacy uses to transfer patient information** so that the Toolkit questions about email will be automatically marked 'complete'.

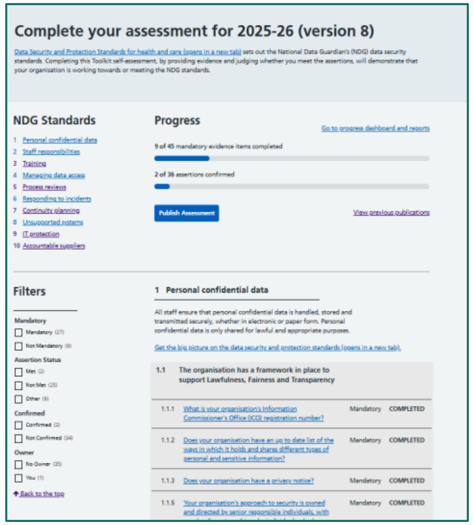
d) **Confirm if you have a Caldicott Guardian** (not mandatory).[3] You can return to the Organisation Profile webpage to update this.

3. Consider whether all staff members have received appropriate training within the past year.

Toolkit question 3.2.1 asks: *"Have at least 95% of all staff completed on data security?"*. The tip links to pharmacy guidance materials such as cpe.org.uk/dstraining. Training can be re-circulated, and staff can sign to confirm that they have reviewed it. Some pharmacy teams also hold annual staff training session to discuss data security matters and identify opportunities for improvement in the coming year. It is essential to ensure that 95% of **all** current staff members have been (re-)trained within the Toolkit period.

4. Consider the Toolkit Parent Organisation Code (POC/HQ) 'batch submission' feature and check the correct pharmacies are listed against your POC

[1] Note: The relevant links are listed at cpe.org.uk/tk if you are using a printed copy of this briefing.
[2] The Toolkit's login page. If you need to register: First register on the Toolkit registration page in sufficient time so that you can complete it before 30th June 2024. You will need an email address (NHSmail or otherwise), your ODS (F) code, and a few minutes for the registration process. Once you have obtained your login credentials login to the Toolkit. The primary user can link other users.
[3] For related guidance see: cpe.org.uk/dsroles



Complete your assessment for 2025-26 (version 8)

Data Security and Protection Standards for health and care (opens in a new tab) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

NDG Standards

1 Personal confidential data
2 Staff responsibilities
3 Training
4 Managing data access
5 Process reviews
6 Responding to incidents
7 Continuity planning
8 Unsupported systems
9 IT protection
10 Accountable suppliers

Progress

Go to progress dashboard and reports

9 of 45 mandatory evidence items completed

2 of 36 assertions confirmed

Filters

Mandatory
□ Mandatory (27)
□ Not Mandatory (9)

Assertion Status
□ Met (2)
□ Not Met (25)
□ Other (9)

Confirmed
□ Confirmed (2)
□ Not Confirmed (34)

Owner
□ No Owner (35)
□ You (1)

Back to the top

1 Personal confidential data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

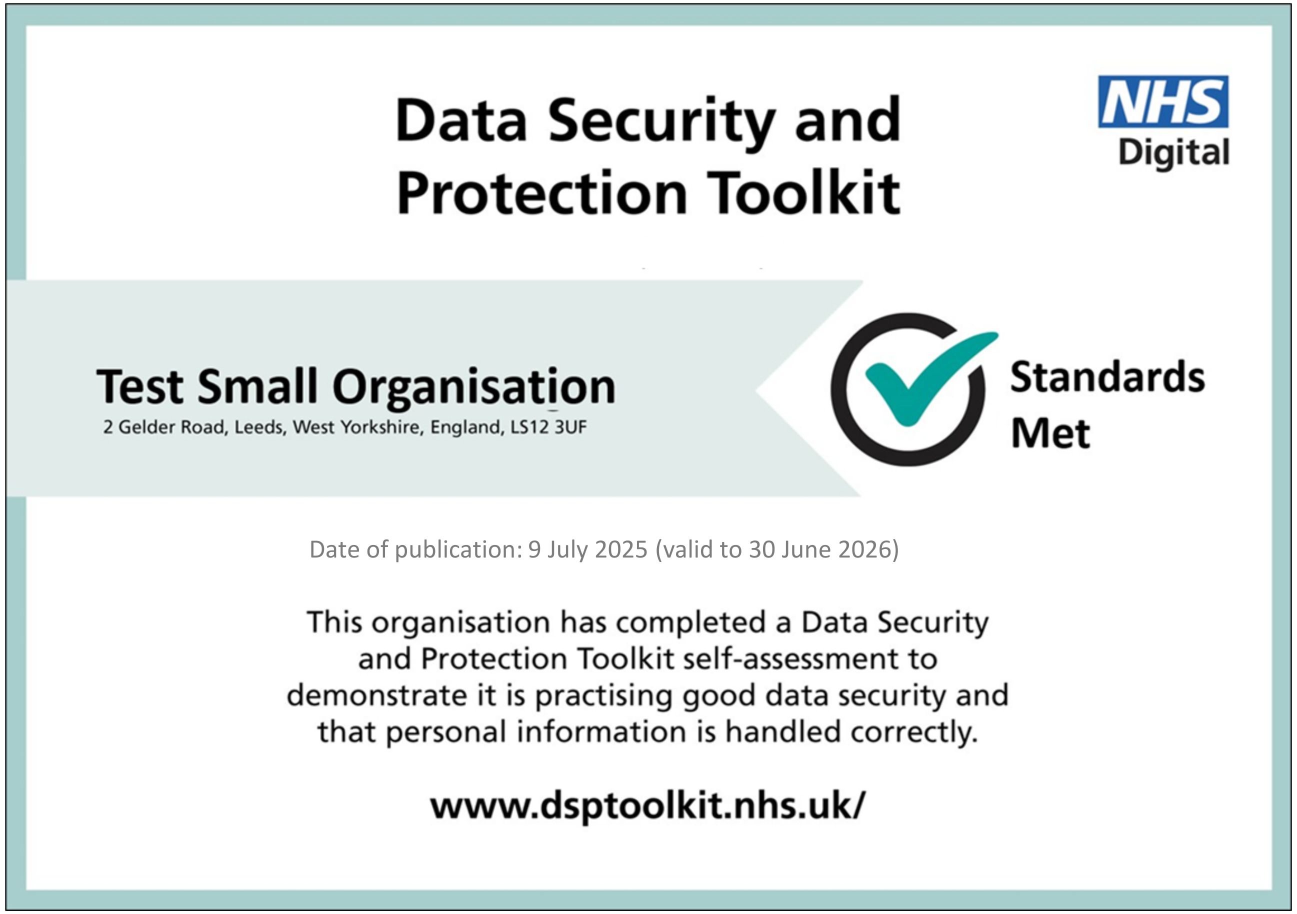
Get the big picture on the data security and protection standards (opens in a new tab).

1.1 The organisation has a framework in place to support Lawfulness, Fairness and Transparency

1.1.1	What is your organisation's Information Commissioner's Office (ICO) registration number?	Mandatory	COMPLETED
1.1.2	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	Mandatory	COMPLETED
1.1.3	Does your organisation have a privacy notice?	Mandatory	COMPLETED
1.1.5	Your organisation's approach to security is owned and directed by senior responsible individuals, with	Mandatory	COMPLETED

DSPTK certificate

- You are now issued with a certificate when you complete the DSP Toolkit.
- This can be shared with branches, commissioners, patients etc.,



NHS Digital

Data Security and Protection Toolkit

Test Small Organisation

2 Gelder Road, Leeds, West Yorkshire, England, LS12 3UF

Standards Met

Date of publication: 9 July 2025 (valid to 30 June 2026)

This organisation has completed a Data Security and Protection Toolkit self-assessment to demonstrate it is practising good data security and that personal information is handled correctly.

www.dsptoolkit.nhs.uk/

Cyber tips

Remote consultations

Use video conferencing to communicate with colleagues, patients and service users if needed.
Read more: cpe.org.uk/rc

NHS Smartcards

Pharmacy staff who regularly work at multiple sites need to have the correct codes on their Smartcard, which can be arranged by the local Smartcard Registration Authority (RA). A good MFA solution option.
Read more: cpe.org.uk/ra

Emails

Be careful of suspicious links or suspicious attachments in emails – don't click on these.
Read more: cpe.org.uk/emailit

Mobile phones

It is permissible to use mobile messaging to communicate with colleagues, patients and service users.
Further information about how to do this safely and securely can be found here: cpe.org.uk/mobilemessages

No faxes

Encourage local health and care colleagues to use NHSmail instead of faxes to contact you.
Read more: cpe.org.uk/fax

Demonstration

Please submit your questions through Slido

Go to **www.slido.com** and enter code **#2785604**.

Or simply scan the QR code.

You may find it helpful to use a separate device e.g. a smartphone.

Questions and answer session

Questions after the webinar can be directed to the support below:

@ Daniel.Ah-Thion@cpe.org.uk
Katrina.Worthington@cpe.org.uk
enquiries@nhsdigital.nhs.uk

Community Pharmacy England

NHS England

Thank you for attending

Post-webinar questions can be directed to the support below:

@ Daniel.Ah-Thion@cpe.org.uk
Katrina.Worthington@cpe.org.uk
enquiries@nhsdigital.nhs.uk