

Data Security and Protection Toolkit Workshop: Introduction

John Hodson

NHS DSPTK team

Katrina Worthington

Regulations Officer

Daniel Ah-Thion

Community Pharmacy IT Policy Manager



In this webinar



- Toolkit submission this year
- Pharmacy guidance
- Multi-factor authentication (MFA)
- 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.



Guidance available

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



Pharmacy-specific Info

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



Publicly shared status

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



GDPR Workbook

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



Supplier support

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



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 2024-25 (version 7)

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

10 of 43 mandatory evidence items completed

2 of 36 assertions confirmed

[Publish Assessment](#)

[View previous publications](#)

Filters

Mandatory

☐ Mandatory (28)

☐ Not Mandatory (10)

Assertion Status

☐ Met (8)

☐ Not Met (20)

☐ Other (5)

Confirmed

☐ Confirmed (2)

☐ Not Confirmed (34)

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	Mandatory COMPLETED

What you need to do (summary)



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



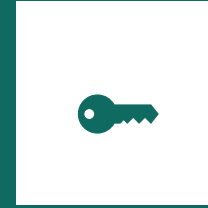
Access the Toolkit

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



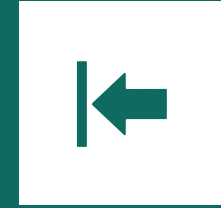
Click the 'Log in' button

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

The screenshot shows the NHS Data Security and Protection Toolkit login interface. At the top, the NHS logo and 'Data Security and Protection Toolkit' are displayed. Below this, there are two main login options: 'Log in with a Data Security and Protection Toolkit account' and 'Log in with NHSmail'. The first option includes fields for 'Email Address' (with the example 'h.hodson@nhs.net') and 'Password', followed by a 'Log in' button and a 'Forgot your password?' link. The second option, 'Log in with NHSmail', includes a 'Log in with NHSmail' button and a note for users who have upgraded their account, with a 'More information' link. Navigation links for 'Organisation search' and 'News' are visible in the top right corner.

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.

The screenshot shows the 'Profile Details' page in the system. At the top, there are navigation links: 'Assessment', 'Report an Incident', and 'Admin'. Below the title 'Profile Details', a warning message states: 'Changing your organisational profile may alter the assertions and evidence you are asked to respond to.' The page is divided into two main sections: 'Sector Information' and 'Key Roles:'. The 'Sector Information' section shows 'Primary Sector' as 'Pharmacy' with a 'Change' link. The 'Key Roles' section lists three roles: 'Caldicott Guardian', 'SIRO', and 'IG Lead'. Each role has a 'Change' link and a table of details. The details for each role are as follows:

Role	Full Name	Email	Telephone	Job Title
Caldicott Guardian	Mr Smith	smith@pharmacy.co.uk	01234 567890	Manager
SIRO	Mr Smith	smith@pharmacy.co.uk	01234 567890	Manager
IG Lead	Mr Smith	smith@pharmacy.co.uk		

Completing your Organisation Profile (2)

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

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

Confirm NHSmal use

Avoid sharing NHSmal logins

Cyber Essentials PLUS

NHSmal 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

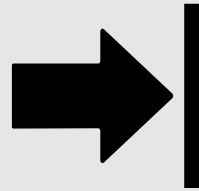
Does your organisation have Cyber Essentials PLUS Certification with a scope covering all health and care data processing awarded during the last 12 months? No [Change](#)

Refreshing the GDPR Workbook



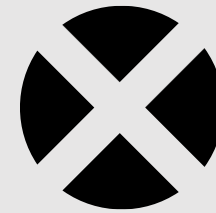
Refresh GDPR Workbook

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



Training log maintenance

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



Data security training

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



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

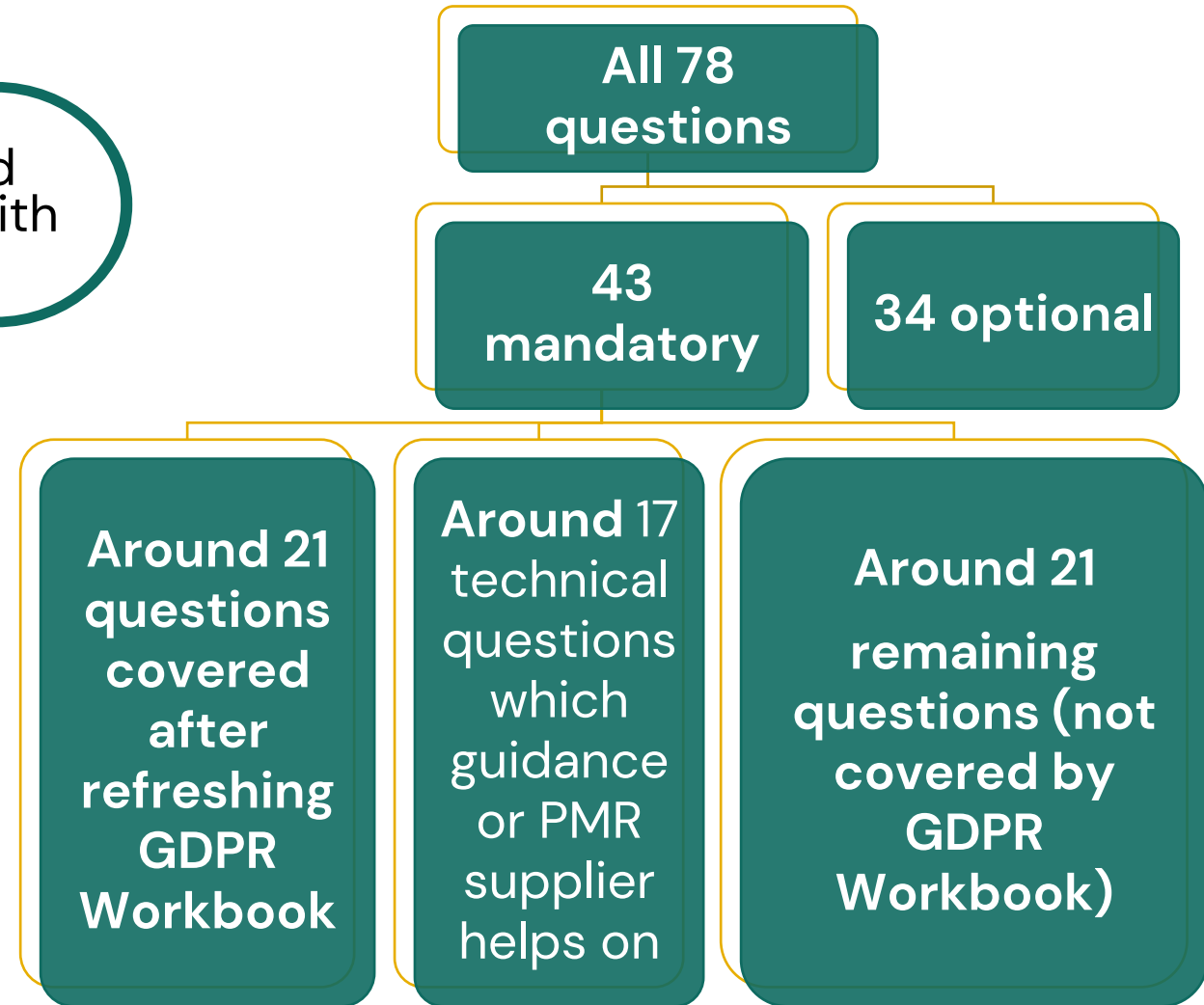
CPE also have specific guidance and a batch submission how-to guide to assist with checking your pharmacies linked to your POC cpe.org.uk/tk.

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



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

[clear filters](#)

Mandatory

- ☒ Mandatory (25)
- ☐ Not Mandatory (11)

Assertion Status

- ☐ Met (11)
- ☒ Not Met (14)

Confirmed

- ☐ Not Confirmed (25)

Owner

- ☐ No Owner (25)

Complete your assessment for 2024-25 (version 7)

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](#)

10 of 43 mandatory evidence items completed

2 of 38 assertions confirmed

[Publish Assessment](#)

[View previous publications](#)

Filters

- Mandatory**
- ☐ Mandatory (26)
- ☐ Not Mandatory (10)

- Assertion Status**
- ☐ Met (8)
- ☐ Not Met (20)
- ☐ Other (3)

- Confirmed**
- ☐ Confirmed (2)
- ☐ Not Confirmed (34)

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 data?	Mandatory COMPLETED

Toolkit question 3.1.1 change

Training needs analysis

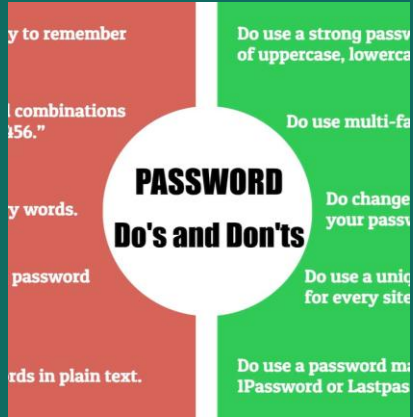


- It involves a thorough assessment of the organization's current and future training requirements, enabling the development of targeted and effective training programs.
- There is a community pharmacy training needs assessment template (cpe.org.uk/dstemplates / cpe.org.uk/dstraining)
- The CP template indicates IG leads can use advanced pharmacy data security materials (e.g. GDPR Part One training), whilst others can use the 'Pharmacy security training refresher' or equivalent.
- This year for the first time, the question will invite you to upload your document or refer to where you store your analysis document

The training needs analysis is a crucial component of ensuring staff have the necessary skills and knowledge to support data protection

Toolkit question tip 4.5.4 change:

Password practice

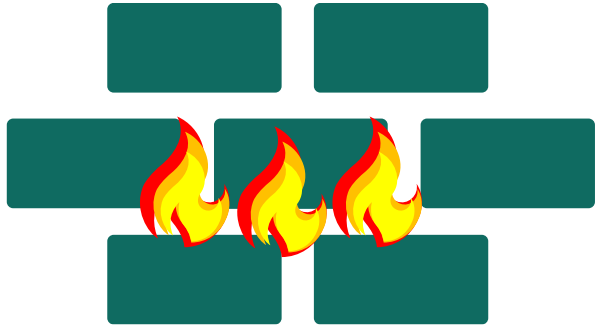


- Good password practice applies not just to hardware, but also to other systems such as clinical web portal systems.
- There is a community pharmacy access control and password procedure template (cpe.org.uk/dstemplates)

“ 4.5.4 updated tip: *If your organisation has any IT systems or computers, it should provide advice for setting and managing passwords. Each person should have their own password/s to access the computer, laptop or tablet that they are using and for other systems. These passwords should be 'strong' i.e. hard to guess. This could be enforced through technical controls i.e. your system(s) require a minimum number of characters or a mixture of letters and numbers in a password...* ”

The password procedure tip has been updated to support secure arrangements

New optional question 9.6.1: Firewall



Firewall Configuration

The optional question relates to ensuring your networks are protected by configuring and maintaining firewalls to control inbound and outbound traffic.

“

Optional question 9.6.1: *“One or more firewalls (or similar network device) have been installed on all the boundaries of the organisation's internal network(s)”*

Tip: *“A firewall is hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.”*

”

Effective firewall management and network security are crucial for protecting your organization's data and systems from cyber threats.

New Toolkit question 4.5.3: Multi-Factor Authentication



New Mandatory Question

The toolkit now includes a new 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 new 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

- **Year one** aim is to encourage organisations to implement MFA
- **Year two** review of results and expect to strengthen requirement over the years

How to answer the MFA question

Scoping

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

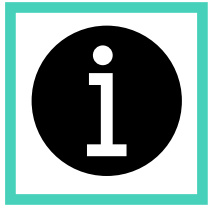
Delivery

- 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

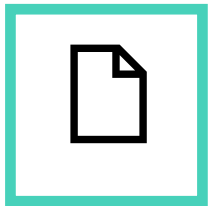
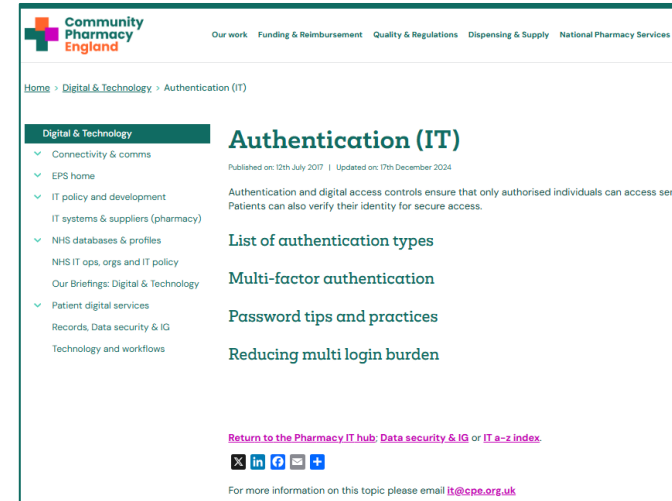
- Recorded for each system
- Approved by board or senior management

MFA support: Community Pharmacy England & NHS England



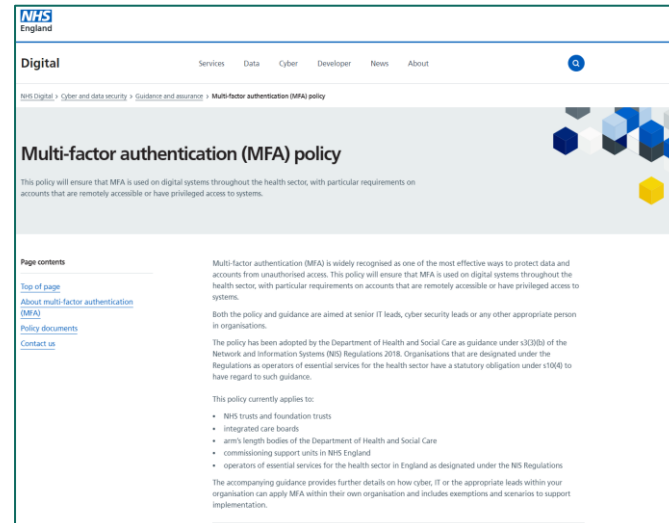
Get MFA guidance from Community Pharmacy England

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



Consider NHS England's MFA policy

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



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.

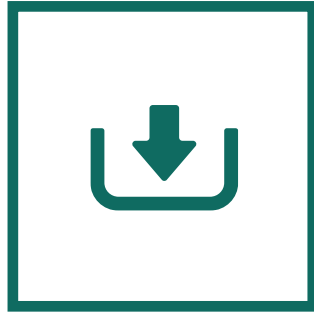
Information from IT suppliers about... (1)

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



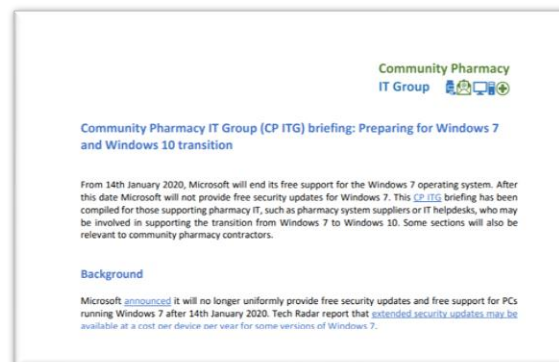
Pharmacy IT updates

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











Windows 10 transition

Review the guidance on cpe.org.uk/windows for a smooth transition to the new Windows 10 operating system in your pharmacy.



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

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.



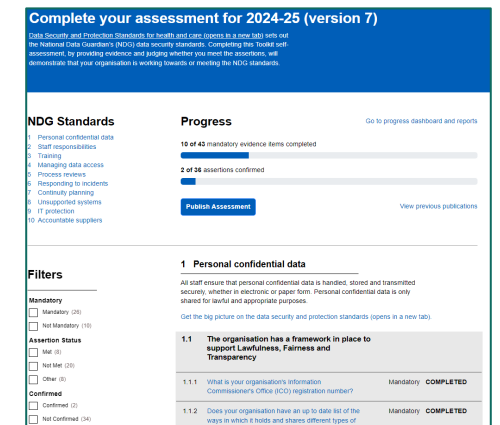
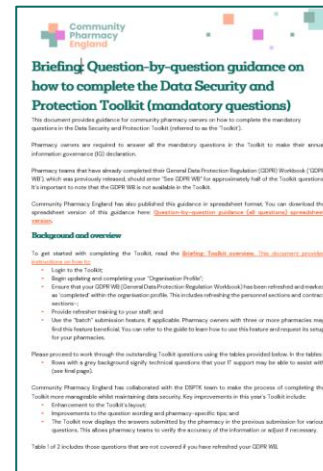
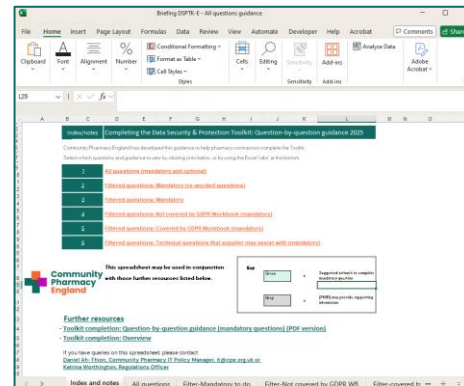
Summarises action and sets out how to do it

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.



DSPTK certificate

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



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



The background is an abstract composition of soft, out-of-focus light spots (bokeh) in shades of blue and purple. Diagonal streaks of light, transitioning from purple to pink, cut across the frame from the top right towards the bottom left. On the left side, there are larger, more complex light patterns that resemble stylized clouds or smoke in light blue and white.

Demonstration



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.



Questions and answer session

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



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