Community Pharmacy England

NHS England

Data Security and Protection Toolkit Workshop: Introduction

Community Pharmacy England

NHS DSPTK team

Data Security and Protection Toolkit Workshop: Introduction

Community Pharmacy England

NHS DSPTK team

- Toolkit submission this year
- Pharmacy guidance
- What’s coming
- Q&A

Community Pharmacy England

NHS England

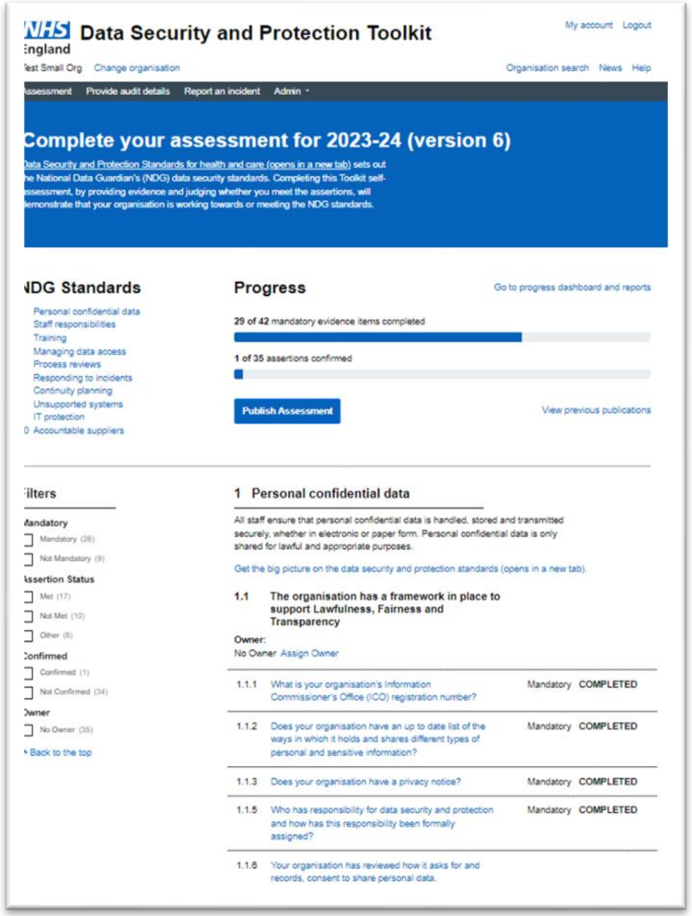
Key Messages

- Toolkit Launched
- Deadline 30th June
- The 'tool tips' include pharmacy specific information
- Community Pharmacy England GDPR workbook if completed means you can confirm 'see GDPR WB' for many questions
- Community Pharmacy England guidance at: cpe.org.uk/ds
- DSPTK status available publicly and shared with NHS England
- Suppliers can help pharmacy IG leads that are completing their DSPTK

Community Pharmacy England

NHS England

What is the Data Security and Protection Toolkit



NHS ngland Data Security and Protection Toolkit

My account Logout

est Small Org Change organisation

Organisation search News Help

omplete your assessment for 2023-24 (version 6)

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

DG Standards

- Personal confidential data
- Staff responsibilities
- Training
- Managing data access
- Process reviews
- Responding to incidents
- Continuity planning
- Unsupported systems
- IT protection
- 0 Accountable suppliers

Progress

Go to progress dashboard and reports

29 of 42 mandatory evidence items completed

1 of 35 assertions confirmed

View previous publications

ilters

andatory

- □ Mandatory (26)
- □ Not Mandatory (9)

ssertion Status

- □ Met (17)
- □ Not Met (10)
- □ Other (8)

onfirmed

- □ Confirmed (1)
- □ Not Confirmed (34)

wner

- □ No Owner (35)

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

Owner:
No Owner Assign Owner

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	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory	COMPLETED
1.1.6	Your organisation has reviewed how it asks for and records, consent to share personal data.		

- Annual online data security self-assessment deadline 30th June
- Enables NHS organisations to measure themselves against the NDG Data Security Standards
- Provides support to comply with GDPR and basic cyber hygiene
- All NHS organisations that process health and care data must complete the Toolkit

Community Pharmacy England

NHS England

What you need to do – summary

- Register if haven't previously
- Review the updated questions
- If you are part of a chain, consider batch submission and check the pharmacy premises listed under your parent org first
- **Publish** – this can be done multiple times before the 30 June deadline if you want to add something or refine an answer

Community Pharmacy England

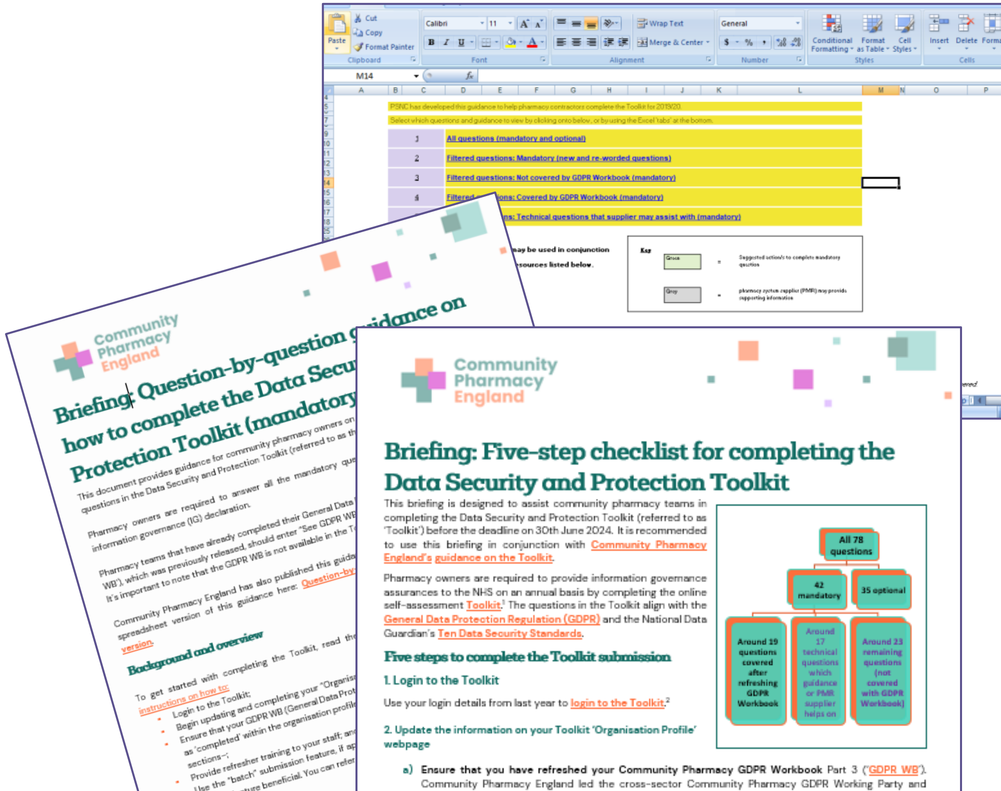
NHS England

Guidance overview

- **Overview briefing**: five steps to complete the Toolkit
- **Question-by-question guidance (mandatory questions)** pdf
  Question-by-question guidance (all questions) spreadsheet

Additional NHS support includes:

- FAQs including Training Tool
- Support available from the Exeter Helpdesk
- Toolkit training and events



PSNC has developed this guidance to help pharmacy contractors complete the Toolkit for 2019/20.

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 (new and re-worded questions)
3	Filtered questions: Not covered by GDPR Workbook (mandatory)
4	Filtered …ions: Covered by GDPR Workbook (mandatory)
	…ns: Technical questions that supplier may assist with (mandatory)

…ay be used in conjunction
…esources listed below.

Key

Green	=	Suggested action/s to complete mandatory question
Grey	=	pharmacy system supplier (PMR) may provide supporting information

Community Pharmacy England

Briefing: Question-by-question guidance on how to complete the Data Secu… Protection Toolkit (mandatory…

This document provides guidance for community pharmacy owners on… questions in the Data Security and Protection Toolkit (referred to as th…

Pharmacy owners are required to answer all the mandatory que… information governance (IG) declaration.

Pharmacy teams that have already completed their General Data… WB'), which was previously released, should enter "See GDPR WB… It's important to note that the GDPR WB is not available in the T…

Community Pharmacy England has also published this guida… spreadsheet version of this guidance here: Question-by… version.

Background and overview

To get started with completing the Toolkit, read the… instructions on how to:

- Login to the Toolkit;
- Begin updating and completing your "Organisa…
- Ensure that your GDPR WB (General Data Prot… as 'completed' within the organisation profile… sections–;
- Provide refresher training to your staff; an…
- Use the "batch" submission feature, if ap… feature beneficial. You can refer…

Community Pharmacy England

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

Community Pharmacy England

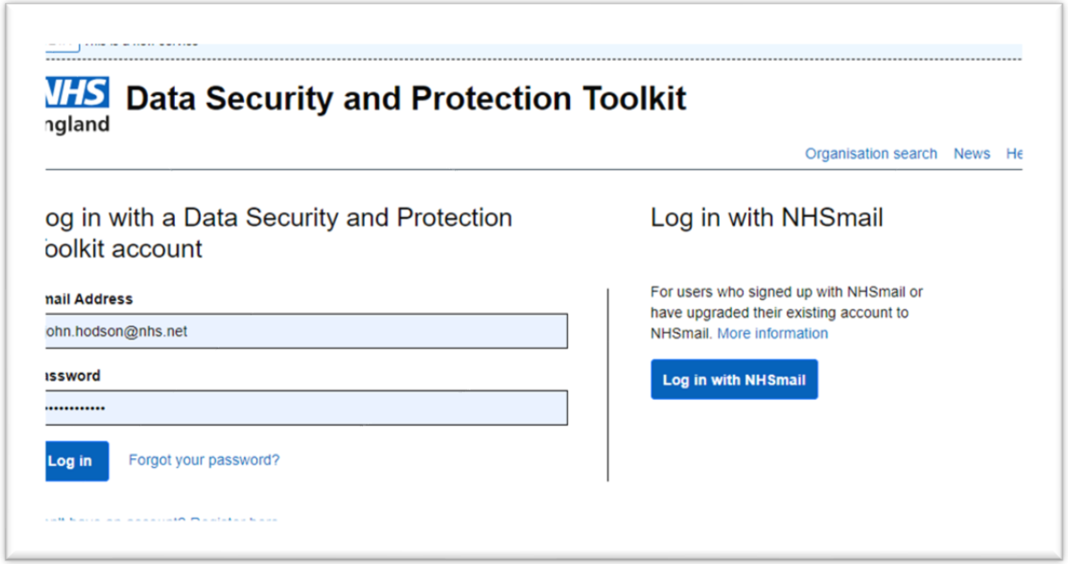
NHS England

1. Login to the Toolkit

- Go to dsptoolkit.nhs.uk

  and click ‘Log in’ on the top right
- Use your login details from last year so previous answers are remembered
- Use ‘Forgot your password?’ option if needed and a reset link will be sent to the email address you registered with

If registration is required, you’ll need an email address (NHSmail or otherwise) and your pharmacy’s ODS code



NHS England Data Security and Protection Toolkit

Organisation search News He

og in with a Data Security and Protection oolkit account

nail Address

ohn.hodson@nhs.net

ıssword

•••••••••••

Log in Forgot your password?

Log in with NHSmail

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

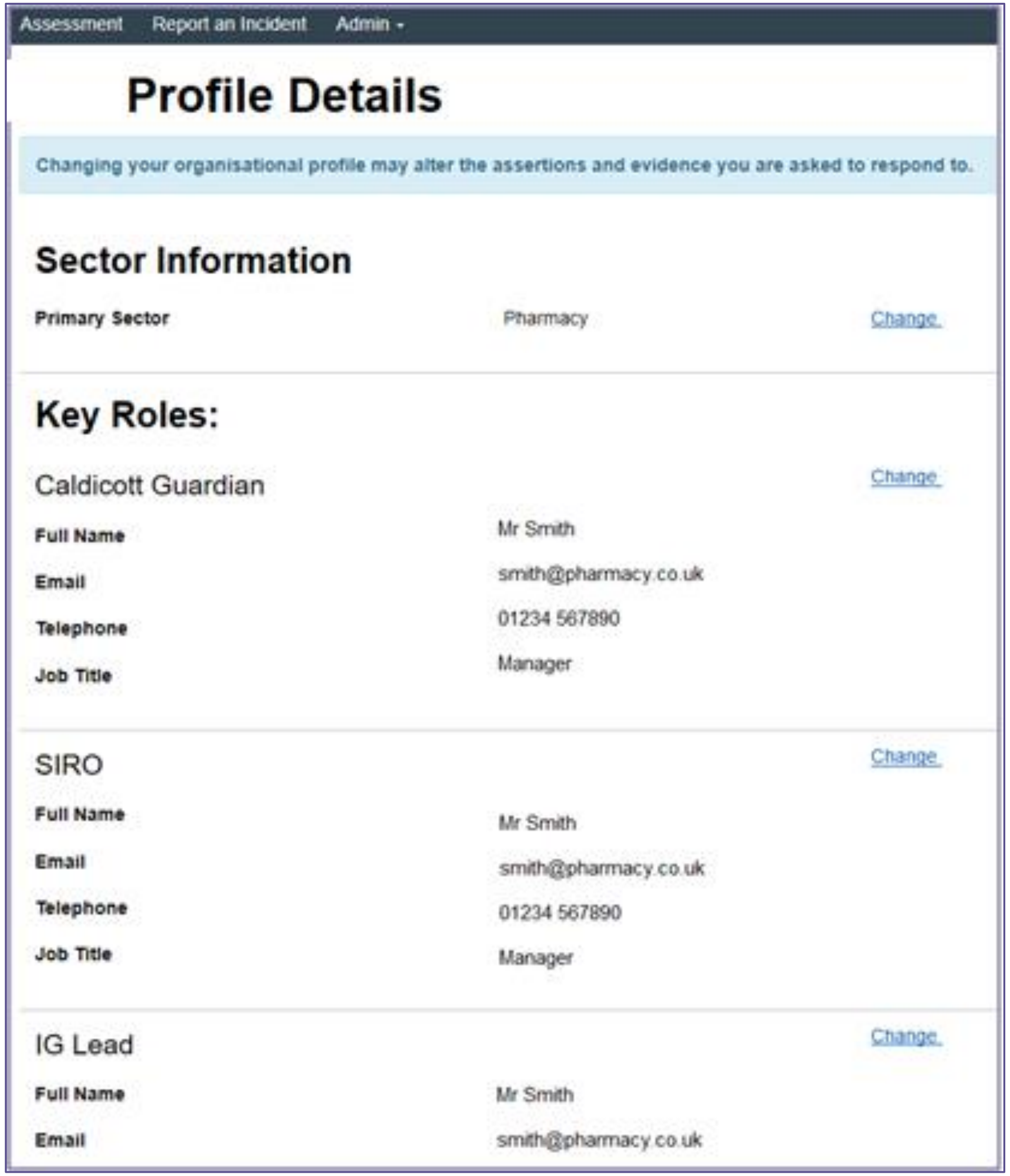
Log in with NHSmail

Community Pharmacy England

NHS England

2. Complete your Organisation Profile

- Enter key roles for the pharmacy, including the Caldicott Guardian, SIRO and IG Lead
- Update any of the contact information if needed



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

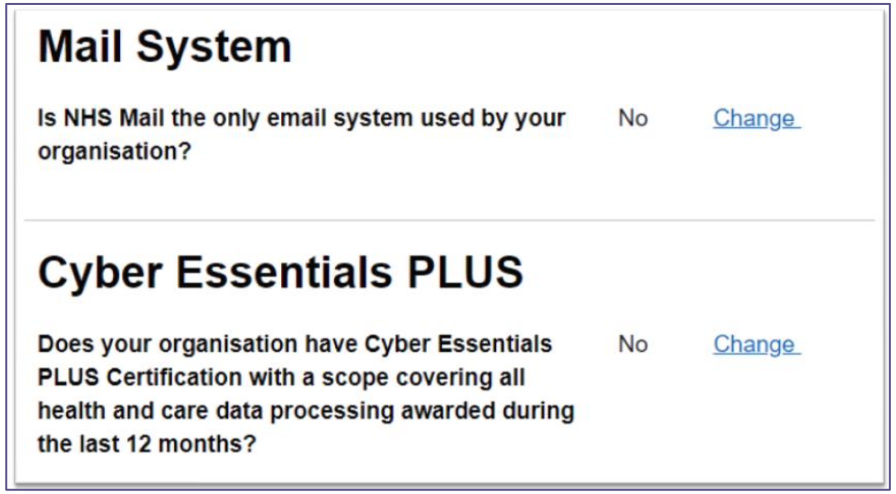
Full Name	Mr Smith
Email	smith@pharmacy.co.uk

Community Pharmacy England

NHS England

2. Complete your Organisation Profile: NHSmail and Cyber Essentials

- NHSmail – the only email system used for sharing patient data
  - The sender and receiver both need NHSmail for fully secure transmission
  - NHSmail login details must not require any sharing amongst staff
- Cyber Essentials PLUS is unlikely to apply to your pharmacy



Mail System

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

Cyber Essentials PLUS

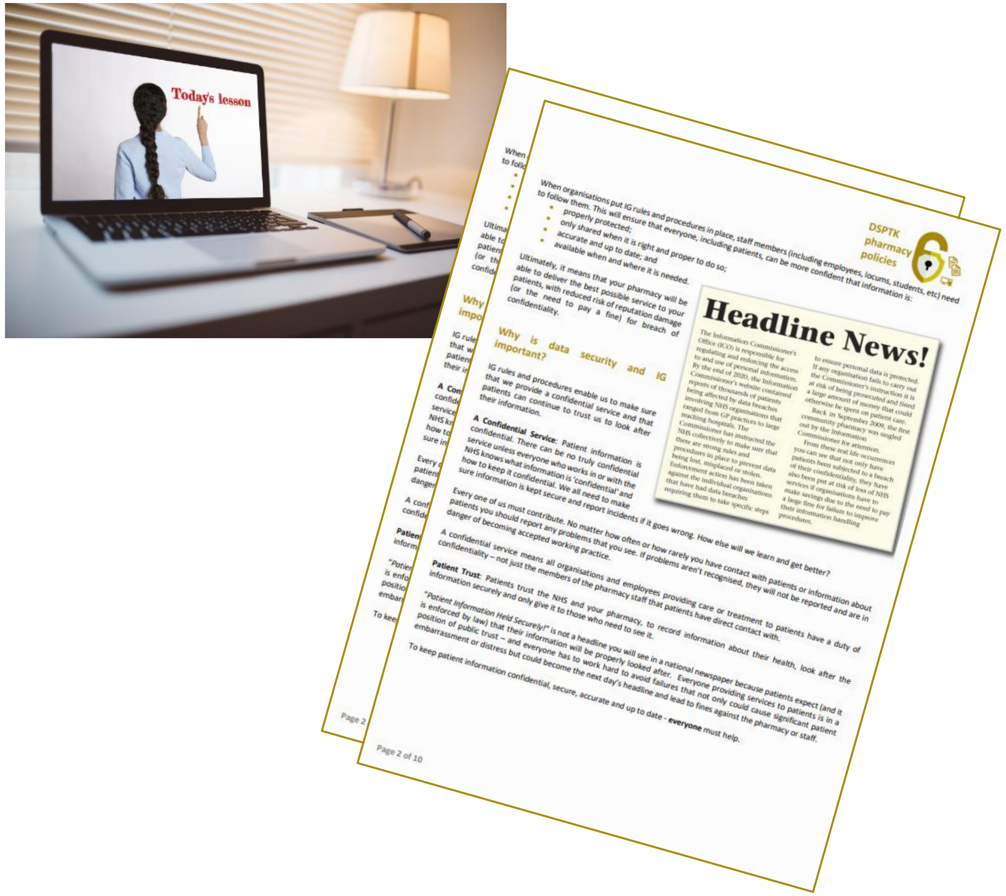
Does your organisation have Cyber Essentials PLUS Certification with a scope covering all health and care data processing awarded during the last 12 months?	No	Change

2. Refreshing the GDPR WB

- How to refresh your GDPR WB
- Refreshing GDPR WB means you can paste ‘See GDPR WB’ into around half of the questions
- Note that the ‘GDPR WB completed’ option is **not** listed anymore within the organisation profile

3. Consider staff training

- Training is required each year for 95%+ of staff
- Critical for mitigating risks and protecting data
- Toolkit Training question (Q3.2.1) references Data Security training:
  - e.g. Pharmacy data security and IG training (for induction or refreshment)
  - e.g. GDPR staff training booklet from Community Pharmacy England meets this
- The training or training log could be re-dated to confirm all staff have gone through it again


Today's lesson
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.

Headline News!

The Information Commissioner's Office (ICO) is responsible for regulating and enforcing the access to and use of personal information. By the end of 2020, the Information Commissioner's website contained reports of thousands of patients being affected by data breaches involving NHS organisations that ranged from GP practices to large teaching hospitals. The Commissioner has instructed the NHS collectively to make sure that there are strong rules and procedures in place to prevent data being lost, misplaced or stolen. Enforcement action has been taken against the individual organisations that have had data breaches requiring them to take specific steps to ensure personal data is protected. If any organisation fails to carry out the Commissioner's instruction it is at risk of being prosecuted and fined a large amount of money that could otherwise be spent on patient care.

Back in September 2009, the first community pharmacy was singled out by the Information Commissioner for attention.

From these real life occurrences you can see that not only have patients been subjected to a breach of their confidentiality, they have also been put at risk of loss of NHS services if organisations have to make savings due to the need to pay a large fine for failure to improve their information handling procedures.

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.

Page 2 of 10

Community Pharmacy England

NHS England

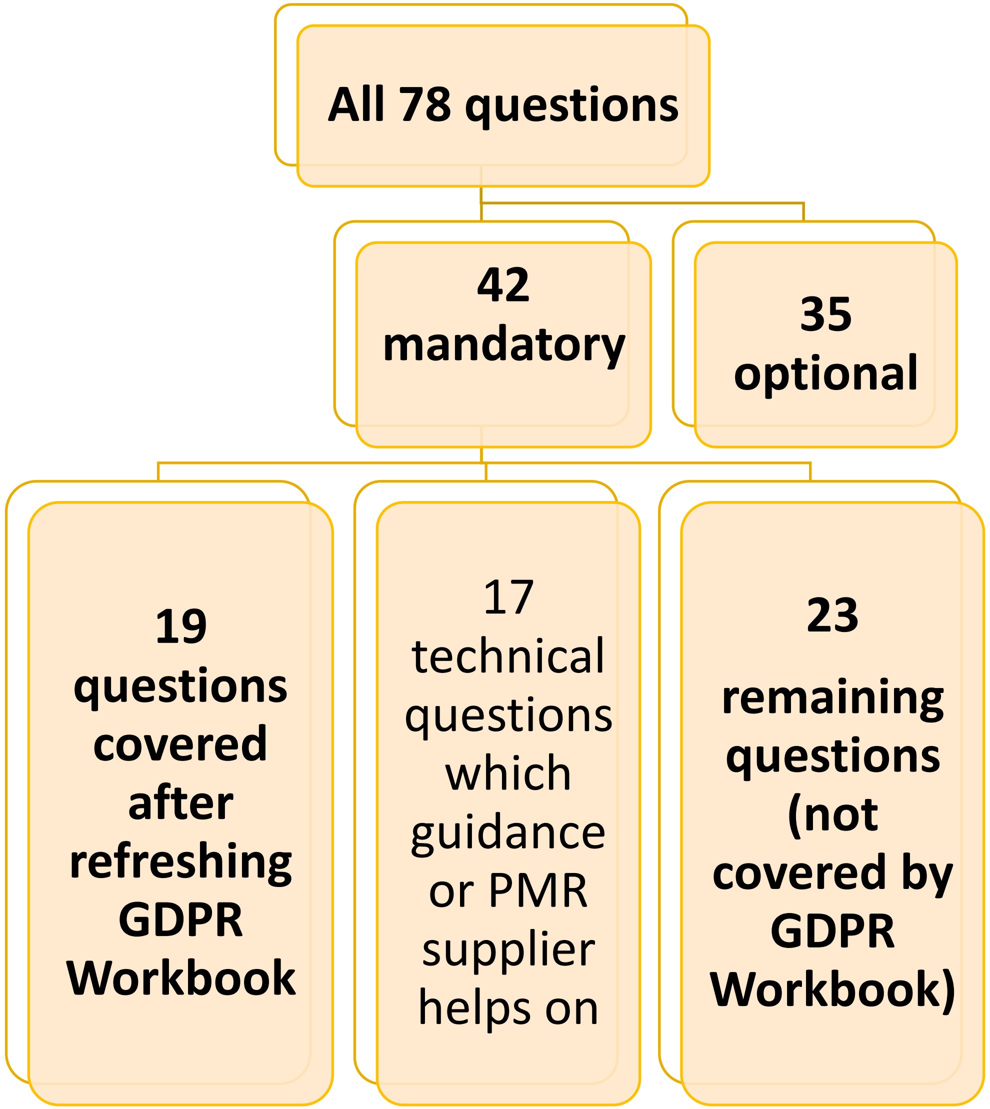
4. The batch submission feature

- For use by pharmacy organisations with three or more pharmacies
- Uses the NHS Parent Organisation Code (POC)
- Allows creation of a single ‘master’ submission for the parent organisation

More will be explained later in the webinar

About the questions

- NHS DSPTK team, Community Pharmacy England, and PMR 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 your GDPR WB
- PMR suppliers may help answer technical questions


All 78 questions

42 mandatory

35 optional

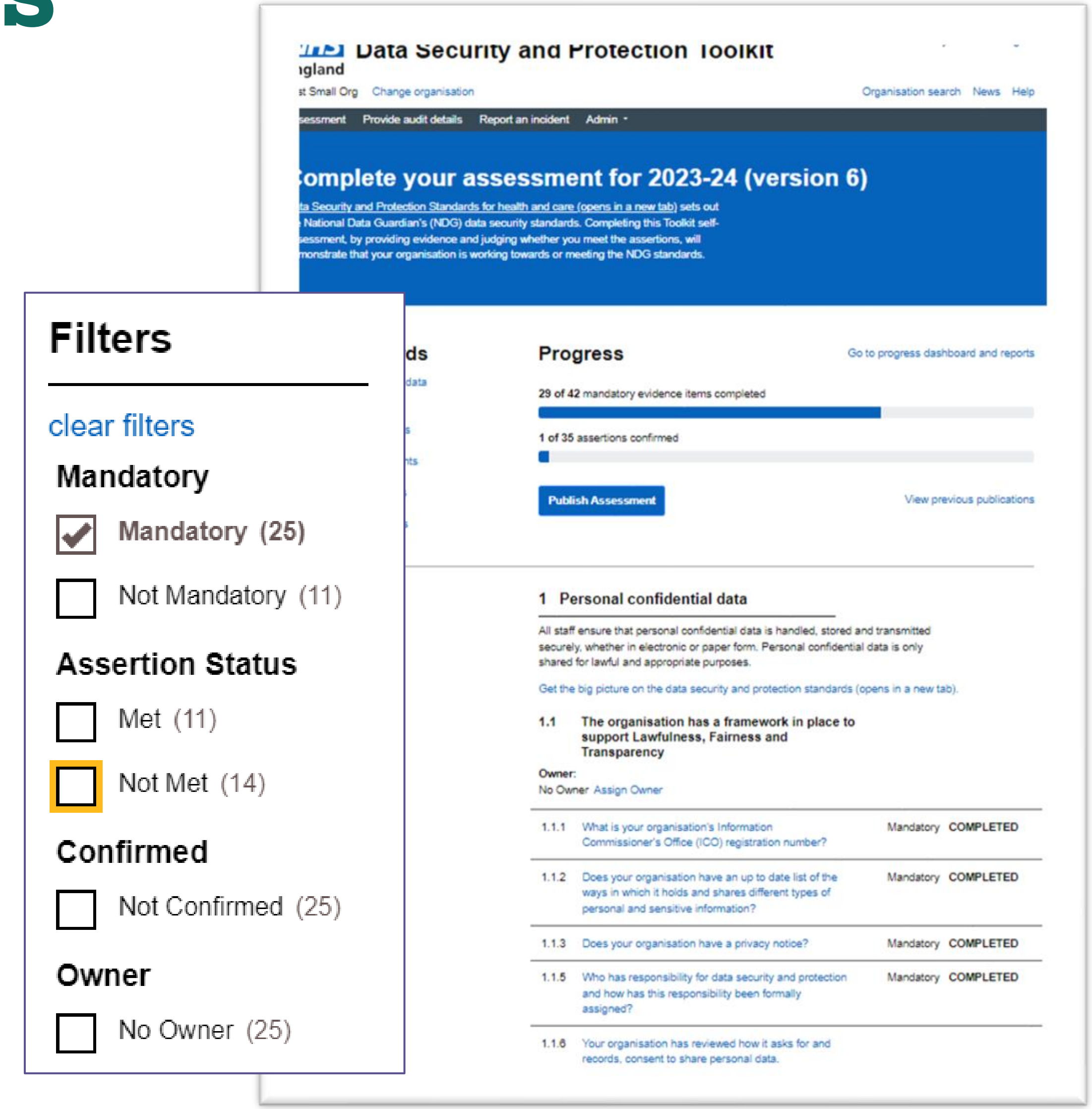
19 questions covered after refreshing GDPR Workbook

17 technical questions which guidance or PMR supplier helps on

23 remaining questions (not covered by GDPR Workbook)

5. Complete remaining mandatory questions

- The ‘optional’ questions do not require completion
- Mandatory questions have the word ‘mandatory’ by their side.
- 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)

Data Security and Protection Toolkit

ıgland

ıt Small Org Change organisation

Organisation search News Help

sessment Provide audit details Report an incident Admin

omplete your assessment for 2023-24 (version 6)

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

Progress

Go to progress dashboard and reports

29 of 42 mandatory evidence items completed

1 of 35 assertions confirmed

Publish Assessment

View previous publications

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).

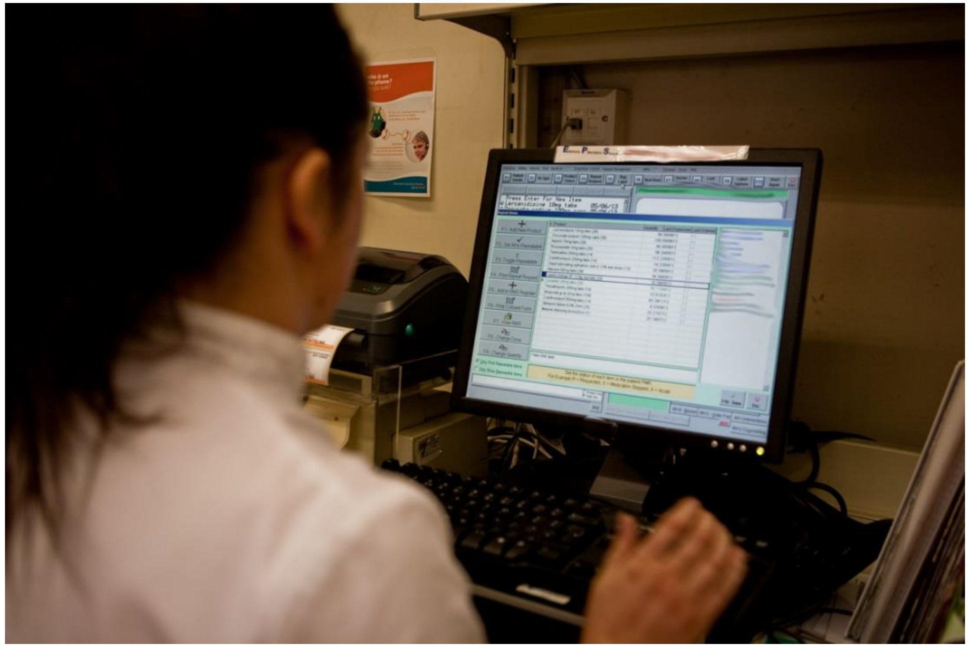
1.1 The organisation has a framework in place to support Lawfulness, Fairness and Transparency

Owner:
No Owner Assign Owner

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	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory	COMPLETED
1.1.6	Your organisation has reviewed how it asks for and records, consent to share personal data.		

Information from your IT suppliers

Some PMR , EPS, CPCF IT suppliers may provide information for pharmacy teams



You might need to ask your IT suppliers about…

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?
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?

You might need to ask your IT suppliers about…

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?

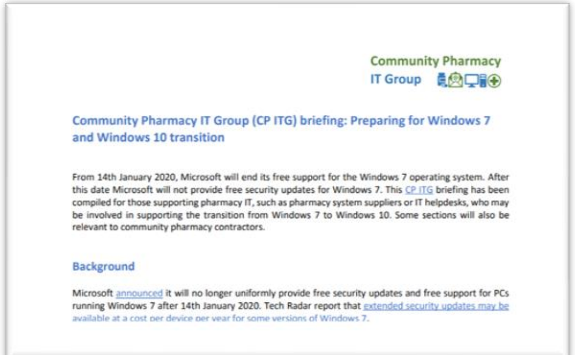
Community Pharmacy England

NHS England

IT updates

- Windows change transitions and guidance

cpe.org.uk/windows



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.

Community Pharmacy England

NHS England

Key Changes this year

- Question on monitoring compliance with policies 1.3.2 has been re-worded the ‘ask’ is much the same
- Assertions and checkboxes are unticked
- Slightly rephrased tooltips with updated CPE links
- Questions and/or tooltips with dates changing to “in the last 12 months"
- Staff Training largest impact

Example question: NHS opt-out system

- Question 1.2.4 asks if the pharmacy aligns with the NHS opt-out policy
- The national data opt-out system offers patients the opportunity to choose for health and care organisations **<u>not</u>** to process data for research / planning
- The opt-out policy does not apply for scenarios such as for processing for patient care purposes
- You may refer to the opt-out system in your Privacy Notice
- Data handlers including PMR suppliers will also confirm within their own Toolkit submissions whether they align with opt-out policy

Example question: Opt-out system

Data flows	Pharmacy data flows reported
Data shared with only 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	✓

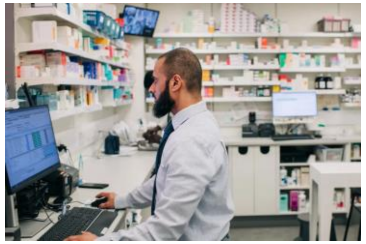
Read more at cpe.org.uk/opt-out and within our question-by-question guidance

Community Pharmacy England

NHS England

Use of NHS GP Connect (NHS Direct Care APIs)

- The Pharmacy First service and potentially additional services over time; will involve pharmacy systems will begin to access record held by the GP, and update the record held by the GP
- GP Connect usage confirmed within MYS
- Suppliers may update privacy notice if required to align with arrangement
- Privacy notice and templates cover use of record information and passing information to other healthcare orgs e.g. GP practices – cpe.org.uk/dstemplates

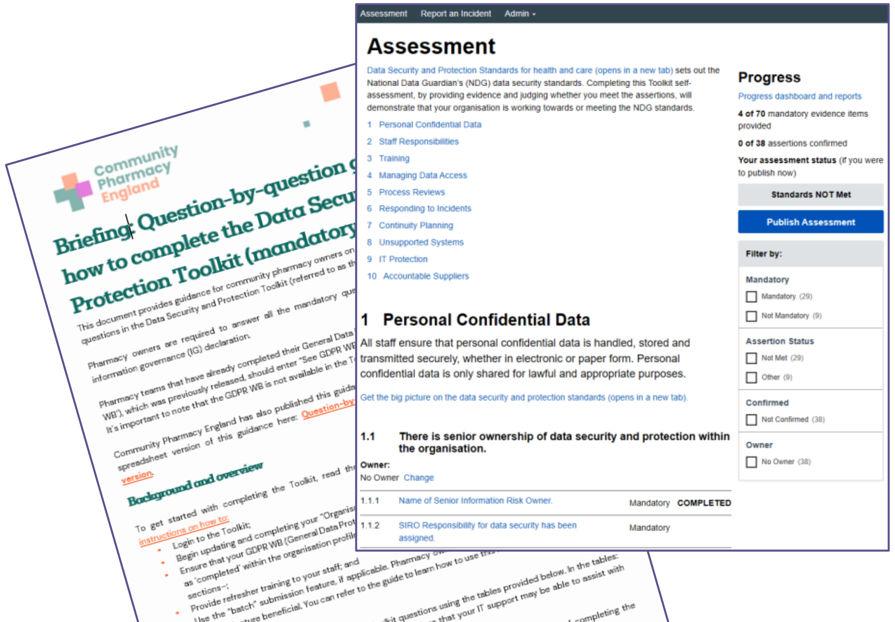


Community Pharmacy England

NHS England

Make use of the question-by-question guidance

- Refer to Community Pharmacy England's question-by-question guidance
- The spreadsheet version can be filtered to display only those questions which are new or have been revised
- Summary actions to take are explained
- Additional templates and info is also provided against each Toolkit question



Community Pharmacy England

Briefing: Question-by-question g
how to complete the Data Secu
Protection Toolkit (mandatory

This document provides guidance for community pharmacy owners on questions in the Data Security and Protection Toolkit (referred to as th

Pharmacy owners are required to answer all the mandatory que information governance (IG) declaration.

Pharmacy teams that have already completed their General Data WB'), which was previously released, should enter "See GDPR WB It's important to note that the GDPR WB is not available in the T

Community Pharmacy England has also published this guida spreadsheet version of this guidance here: Question-by version.

Background and overview

To get started with completing the Toolkit, read the instructions on how to:

- Login to the Toolkit;
- Begin updating and completing your "Organis
- Ensure that your GDPR WB (General Data Prot as 'completed' within the organisation profil sections–;
- Provide refresher training to your staff; and
- Use the "batch" submission feature, if applicable. Pharmacy ow feature beneficial. You can refer to the guide to learn how to use this

kit questions using the tables provided below. In the tables: that your IT support may be able to assist with completing the

Assessment

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.

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

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 There is senior ownership of data security and protection within the organisation.

Owner:
No Owner Change

1.1.1	Name of Senior Information Risk Owner.	Mandatory	COMPLETED
1.1.2	SIRO Responsibility for data security has been assigned.	Mandatory	

Progress

Progress dashboard and reports

4 of 70 mandatory evidence items provided

0 of 38 assertions confirmed

Your assessment status (if you were to publish now)

Standards NOT Met

Filter by:

Mandatory
□ Mandatory (29)
□ Not Mandatory (9)

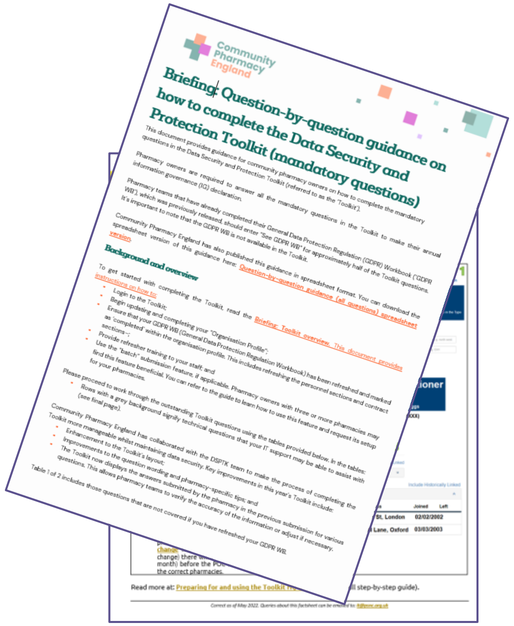
Assertion Status
□ Not Met (29)
□ Other (9)

Confirmed
□ Not Confirmed (38)

Owner
□ No Owner (38)

Getting ready to use the batch feature

- Community Pharmacy England guidance documents on the NHS Parent Organisation Code (POC) HQ batch feature:
    - **Using the POC batch feature step-by-step guide**
    - **Checking pharmacies linked to POC using ODS portal**
- All using it, may check the right pharmacies are linked with the POC code



Community Pharmacy England

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.

Read more at: Preparing for and using the Toolkit ... ll step-by-step guide).

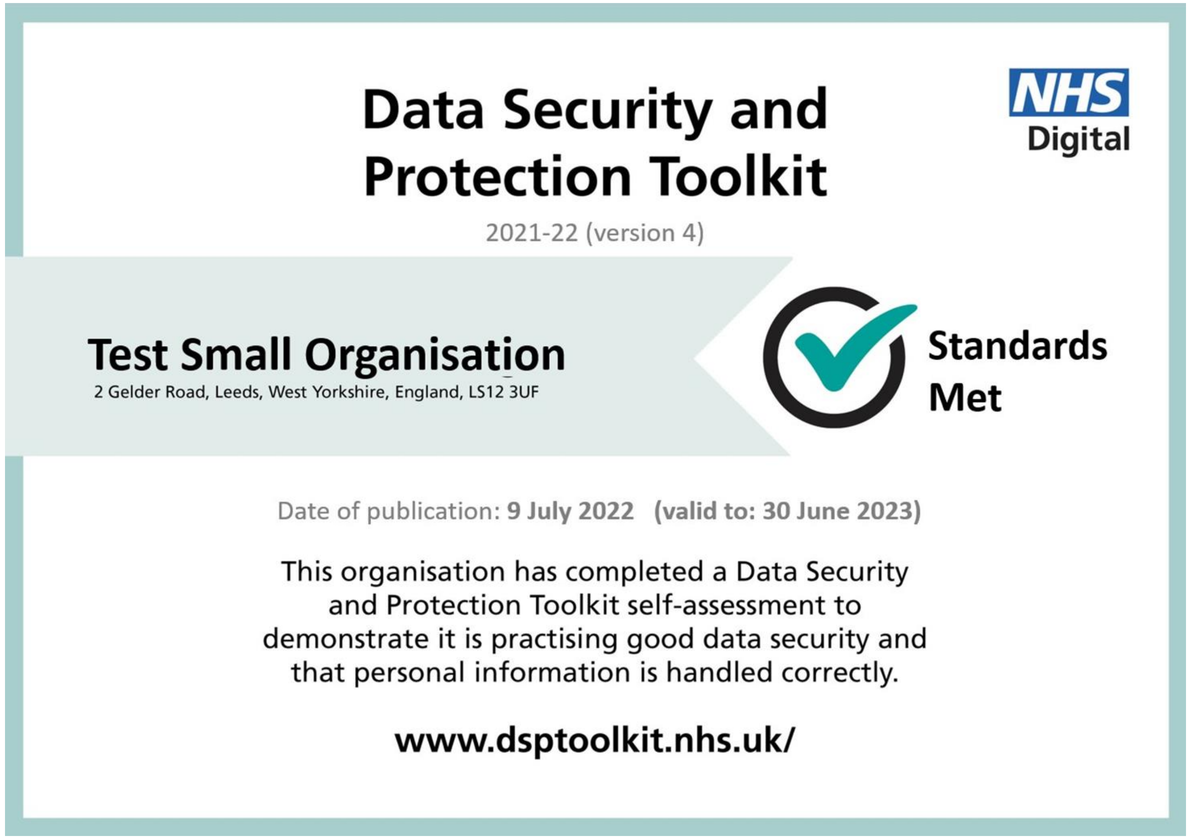
Correct as of May 2022. Queries about this factsheet can be emailed to: it@psnc.org.uk

Community Pharmacy England

NHS England

New function Certificate

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



NHS Digital

Data Security and Protection Toolkit

2021-22 (version 4)

Test Small Organisation

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

Standards Met

Date of publication: **9 July 2022** **(valid to: 30 June 2023)**

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/

Key IT Suppliers move to CAT1

- Additional requirement for large IT suppliers
- Same requirements as an NHS Trust
- Tooltips make clear if individual evidence items are not applicable (i.e. clinical coding for IT Suppliers)
- Only larger IT suppliers (over 50 staff and £10 million turnover)
- Audit voluntary in 23-24.

Using cyber technology: top 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).
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:
Read more: 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

Community Pharmacy England

NHS England

Demonstration

Questions and answer session

If you have questions later, email:

it@cpe.org.uk , Daniel.Ah-Thion@cpe.org.uk , katrina.worthington@cpe.org.uk or enquiries@nhsdigital.nhs.uk

Community Pharmacy England

NHS England