Briefing DS23B: Question-by-question guidance on how to complete the Data Security and Protection Toolkit 2025 (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.

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.

Table 2 of 2 (pages 10-12) provides guidance for the other mandatory questions for pharmacy teams that have not completed or refreshed the GDPR WB.

Question-by-question guidance table 1 of 2

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
1.2.4 - Is your organisation compliant with the national data opt-out policy?	▪ Confirm by ticking if the two following reasons apply (see also cpe.org.uk/optout, which explains this issue in more detail). 1. **Pharmacy teams should include a reference to the opt-out policy within their privacy notices. These privacy notices should be available on their websites and/or provided to patients through leaflets when requested. You should include a reference to the opt-out system in your privacy notice.** The Community Pharmacy England privacy notice template (available at cpe.org.uk/dstemplates Template 5) already includes a mention of the opt-out system: "*You may choose to opt out of the NHS using your data for planning and research purposes – please ask for details.*". If you are not using this template, you can add this clause to the wording of your privacy notice. Additionally, there is a separate question in the Toolkit that asks you to confirm the presence of a privacy notice. 2. **Pharmacy teams will not need to process identifiable patient data with 'planning or research' as the purpose.** **About the opt-out system**: It provides patients with the ability to express their preference regarding the processing of their personally identifiable information by health and care organisations.	**Additional resources**: The Template 5 "Privacy notice" (cpe.org.uk/dstemplates) includes a reference to the opt-out system: "[You may choose to opt out of the NHS using your data for planning and research purposes – please ask for details.]". This opt-out briefing further explains how to complete this question and provides some background information. Pharmacy teams are advised to signpost patients who ask about opt-out to one of the patient-facing options on the left. Community Pharmacy England and the Community Pharmacy IT Group assessed community pharmacy data flows concerning the opt-out system. They concluded that these data flows are not necessary for planning/research, but they are processed for other reasons, such as legal obligations (e.g. Pharmacy Terms of Service) and healthcare. Non-healthcare personal data processed for marketing purposes may require consent. PMR suppliers and the aggregator companies they collaborate with may process data for the pharmacy. These companies should also complete the Toolkit, including the opt-out question. PMR suppliers, aggregators and others may refer to NHS opt-out guidance. Community Pharmacy England plans to list those PMR systems and aggregators that have confirmed compliance with the opt-out system here: cpe.org.uk/optout. Note: This is a question that your PMR pharmacy system supplier or IT support may be able to help you answer (see the FAQ at the end of this document). * Where records are kept electronically, a paper copy of the same information does not need to be stored. For electronic records, there are alternatives to simply keeping or deleting a record, e.g., archiving or 'hiding' from typical system usage – if appropriate. Archiving should be performed with care to protect the patient's	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
	The primary purpose for this is for *Research or planning purposes*, such as improving treatments or enhancing the delivery of health services. Patients can learn more about the opt-out system and express their preferences by:: ▪ Visiting the NHS.uk/yournhsdatamatters website portal; ▪ Using the NHS App; ▪ Sending a written request by post using the instructions at the NHS.uk website; or by ▪ Contacting the NHS contact centre - 0300 303 5678 (open workdays Monday-Friday, 9 am-5 pm).	interests (i.e., the pharmacy team may need to review older information later in some scenarios when providing direct care). The Specialist Pharmacy Service (SPS, sps.nhs.uk) has produced a detailed example record-keeping document for pharmacy teams. **Previous communications to patients**: Patients were previously informed by NHS England that their opt-out preference would be honoured by health and care organisations **by 2021 or before**. NHS England's Transformation Directorate (NHSE's TD) granted organisations an extra extension beyond this. Patients have been notified about the opt-out via NHS transparency notices.	
1.3.12 - How does your organisation ensure that paper records are safe when taken out of the building?	▪ Pharmacy teams could enter that "Materials with identifiable information remain under the supervision of the relevant staff member and are not left unattended within vehicles for long periods, and that most clinical paperwork will be kept within the pharmacy" if this is the case. Delivery drivers and pharmacy staff might need to process limited data outside the pharmacy when necessary and appropriate. Policies and templates can provide guidance and support for off-site processing (see notes).	▪ Template 3 Staff confidentiality code, Template 2 Staff confidentiality agreement and Template 1 Data security policy includes passages about remote working. ▪ Most pharmacy teams will not process patient-identifiable information outside of the pharmacy. Some pharmacy teams have a policy outlining the precautions to be taken when processing data outside the pharmacy. ▪ These precautions include: – avoid leaving paperwork unoccupied in a car in case of motor theft – placing paperwork within an envelope or folder and labelling it with advice to 'contact person x if found'.	☐
1.3.14 - What does your organisation have to minimise the risks if mobile phones are lost,	▪ Pharmacy teams can include the statement "staff mobile phones do not store patient identifiable data" if this is the practice followed. Pharmacy teams should utilise the	▪ Policies, guidance and templates available for pharmacy teams include: cpe.org.uk/mobiledevices ▪ Template 8A "Portable Computer Device Guidelines "Template 8B "Bring Your Own Device Policy and Guideline "Template 9 "Portable equipment control form" to support	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
stolen, hacked or misused?	mobile device policies and templates (see notes). ▪ Alternatively, pharmacy teams can include the statement "Our organisation's policies encompass the use of mobile devices and relevant safeguards" if this is the case (see notes). ▪ If your organisation does not use any mobile phones, write "Not applicable" in the text box. Guidance is available for **pharmacies**.	the maintenance of records Template 6, "Asset Register", enables logging mobile devices and associated information about them.	
1.4.2 – If your organisation uses third parties to destroy records or equipment that holds personal data, is there a written contract that has been reviewed in the last twelve months? This contract should meet the requirements set out in data protection regulations.	▪ Confirm that "Suitable disposal procedures are in place" if this is the case.	Information about the Pharmacy disposal procedures is available at: ▪ Template 4 "Data handling, record keeping and disposal procedures" ▪ cpe.org.uk/dsdispose ▪ Template 22 "List of suppliers that process data"	☐
1.4.3 – If your organisation destroys any records or equipment that holds personal data, how does it ensure this is done securely?	▪ Confirm that "Suitable disposal procedures are in place" if this is the case.	Information about the Pharmacy disposal procedures is available at: ▪ Template 4 "Data handling, record keeping and disposal procedures" ▪ cpe.org.uk/dsdispose ▪ Template 22 "List of suppliers that process data"	☐
2.1.1 – Does your organisation have an induction	▪ Confirm whether appropriate induction training on data security and protection is provided to all new staff.	Those who refreshed the GDPR WB should provide refresher training to all staff. If you have not refreshed the GDPR WB this year, note that the recommended training options include:	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
process covering data security, protection, and cyber security?	▪ Tick and save.	▪ Template 3B "Pharmacy data security and IG training (for induction or refreshment)" (cpe.org.uk//dstrainingrefresher); ▪ "GDPR Guidance for Community Pharmacy (short version) (Part 2) staff training booklet" (see cpe.org.uk/dstraining); ▪ NHS England Data security awareness level 1 (see cpe.org.uk/dstraining); or ▪ equivalent (see cpe.org.uk/dstraining). New joiners should sign the Template 14 staff signature list (cpe.org.uk/dstemplates) after arrival, and all existing staff should sign this annually to confirm their re-training. See the other training questions for more information.	
3.1.1 – Has a training needs analysis covering data security, protection, and cyber security been completed in the last twelve months?	▪ Complete the Template 3D "Training options and analysis". Generally pharmacy IG lead(s) should have more detailed yearly training (GDPR Guidance (Part 1) at cpe.org.uk/dstraining) whilst all other staff should receive at least basic level data security training (e.g. Template 3B "Pharmacy data security and IG training (for induction or refreshment)" (cpe.org.uk/dstrainingrefresher)) ▪ Tick and save once the training needs analysis has been completed.	See: cpe.org.uk/dstraining. A pharmacy training analysis document is at: https://cpe.org.uk/dstraining: Template 3D "Training options and analysis". The organisation's 'training needs analysis' considers the pharmacy's data security and training needs and how these can be met. You can decide what level of training on data security and protection is required for staff grades or roles. You are responsible for ensuring that staff members complete this training. There should be an assessment for all staff (this assessment confirms that every staff member has or will be re-trained with the support of one of the following recommended training options: ▪ the Template 3B "Pharmacy data security and IG training (for induction or refreshment)" (cpe.org.uk/dstrainingrefresher); ▪ "GDPR Guidance for Community Pharmacy (short version) (Part 2) staff training booklet" (see cpe.org.uk/dstraining); ▪ NHS England Data security awareness level 1 (see cpe.org.uk/dstraining); or ▪ equivalent (see cpe.org.uk/dstraining). The IG lead person(s) should undertake more detailed training, e.g., GDPR Guidance (Part 1) (see question 3.4.1, which relates to training for IG leads and cpe.org.uk/dstraining 'IG lead training' section). All staff require annual re-training (see question 3.2.1). Some staff may receive ad hoc training throughout the year, e.g., discussions or memos about good data security practices. Support organisations like	

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
		Community Pharmacy England may also issue data security best practice information. It is suggested that you keep an internal record of training session dates or dates that staff confirm they have reviewed training materials. New staff should undergo a data and security training induction shortly after arrival.	
3.2.1 – Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security, protection, and cyber security in the last twelve months?	▪ Confirm whether at least 95% of all staff have been trained using the "Pharmacy data security and IG training (for induction or refreshment)" or "GDPR Guidance for Community Pharmacy (short version) (Part 2) staff training booklet" or equivalent (see notes). ▪ Tick and save.	Appropriate training includes: ▪ Template 3B "Pharmacy data security and IG training (for induction or refreshment)" (cpe.org.uk//dstrainingrefresher); ▪ "GDPR Guidance for Community Pharmacy (short version) (Part 2) staff training booklet" (see cpe.org.uk/dstraining); ▪ NHS England Data security awareness level 1 (see cpe.org.uk/dstraining); or ▪ equivalent (see cpe.org.uk/dstraining). Ensure that 95% or more of all current staff (including delivery drivers) have completed such training or equivalent. For a small pharmacy, this is likely to be the entire pharmacy team.	☐
3.4.1 – Have the people responsible for data security and protection received training suitable for their role?	▪ Tick and save if this is true.	This confirms that the person(s) with IG lead responsibility and any other leaders and company directors have completed the advanced training appropriate to their roles. Advanced training includes GDPR and data security and protection (see cpe.org.uk/dstraining 'IG lead training' section).	☐
4.1.1 – Does your organisation have an up-to-date record of staff and volunteers, if you have them, and their roles?	▪ Tick and save if this is true.	Confirm that this record is maintained.	☐
4.2.4 – Does your organisation have a reliable way of removing or amending people's access to IT systems when	▪ Tick and save once you are confident about the method; only current staff can access critical IT systems.	You may keep a list of current staff that needs IT rights using cpe.org.uk/dstemplates: Template 6 "Asset register" or Template 14C "List of staff and IT rights". Template 15, "Access control, passwords & accounts procedures", will assist processes within the pharmacy. Template 13, "Audit spot checks", will also help check that leavers IT rights have been revoked.	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
they leave or change roles?		Additional background information: ▪ Some information can be accessed only from within the system. ▪ Smartcards that are not used at all become locked. ▪ Personal NHSmail accounts that are not used for a period become deactivated.	
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.	▪ *Verify MFA usage*: Confirm all staff use multi-factor authentication (MFA) for all clinical IT systems.	▪ *Update templates*: Update Template 14C "List of staff and IT rights" and/or Template 6 "Asset register" to reflect pharmacy staff MFA usage in clinical IT systems. ▪ *Document exceptions*: If MFA is not used by all staff for all clinical IT systems, document the reasons for this within the asset register, the list of systems or in the DSPTK 4.5.3 comments field. Additional background information: ▪ Find out more at our MFA webpage: cpe.org.uk/mfa ▪ Clinical IT systems include: your EPS system, your pharmacy IT services system, use of NHSmail and potentially a patient app and its back-end system. ▪ EPS systems with NHS Smartcards or NHS Care Identity Service profiles meet MFA requirements. ▪ Some systems function only with local computer terminals, also fulfilling MFA requirements. Many of the other updated template documents (cpe.org.uk/dstemplates) also encourage good MFA practices such as: ▪ Template 15, "Access control, passwords & accounts procedures". ▪ Template 8B "Bring Your Own Device Policy" states that personal smartphone devices may be used for authentication purposes, where required.	☐
4.5.4 - How does your organisation ensure that staff, directors, trustees and volunteers use good password practices?	▪ Tick and save if all staff are familiar with good password practice. It is expected that this topic has been covered in the refresher staff training. ▪ Staff can be trained or refreshed on password practices - see Explanatory notes for further details.	For materials that inform staff about good password practices, see cpe.org.uk/passwords and cpe.org.uk/dstraining. The following template documents (cpe.org.uk/dstemplates) also encourage good password practices: ▪ Template 15, "Access control, passwords & accounts procedures", will assist processes within the pharmacy. ▪ Template 2 "Staff confidentiality agreement" ▪ Template 3A "Staff confidentiality code"	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
	▪ Staff may have signed agreements to confirm following appropriate password practices when they joined the organisation.	▪ Templates 14A/B "Staff signature lists"	
5.1.1 – If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?	▪ In case of no security breach, insert "N/A" in the free text box provided. ▪ If there has been a data security breach (e.g., a loss of electronic data, the loss of a prescription bundle, a virus impacting the ability for the pharmacy team to view PMR terminals, etc.), then you should review your use of processes to improve how they are implemented, manage risks, and reduce the likelihood of reoccurrence. ▪ Confirm in the free text box that this process review has been carried out, when this took place, the identified issues, and how the process has been improved to reduce the likelihood of reoccurrence. ▪ Confirm 'save'	A review of data security problems, including near misses or breaches, should be carried out at least once a year. Pharmacy teams are advised to use the following resources when conducting a review: Template 11, "Incident management procedures", and where needed, Template 12 ", Incident report form (data security)" (which are both available at cpe.org.uk/dstemplates). If a data security incident occurs, there is an option to list the incident within the Data Security and Protection Toolkit 'Report an Incident' option within the menu band. NHS England can pass the required information to the Information Commissioners Office (ICO), where necessary. GDPR WB Template I "Consider Data Breaches" of the GDPR WB includes: any notification to the Information Commissioners Office (ICO) must describe the nature of the breach, such as the number of data subjects, records and what was lost, e.g., a prescription; the name and contact details of the DPO; probable consequences of the breach, and measures you have taken, for example, to mitigate any adverse effects. Information that it is impossible to provide immediately should be delivered later without delay. A review of processes may be appropriate after any data breach or near miss in case adjustments can be made to people and processes to reduce the risk of a repeat incident. See also question 6.1.1.	☐
6.2.1 – Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?	▪ Tick and save if antivirus software includes the pharmacy devices that process patient data.	Antivirus protection is essential to protect the pharmacy system from viruses that can compromise data. If you are unsure what anti-virus software is used, check this or contact your IT support. Note that some devices may come with pre-installed antivirus software. Additional guidance is available at: cpe.org.uk/antivirus.	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
		Note about this technical question: this is a question that your IT system suppliers or IT support may be able to help you answer (see FAQ at the bottom of this document). *	
6.3.2 – Have staff, directors, trustees and volunteers been advised that using public Wi-Fi for work purposes is unsafe?	▪ Tick and save if all staff know that accessing sensitive work data over a public WiFi network is inappropriate (see notes for supporting information). ▪ Tick and write 'N/A' in the comments box if no staff use mobile devices for work reasons whilst away from the pharmacy.	Many pharmacies are introducing 'Mobile device and Bring Your Own Device' policies because NHSmail can be accessed on work and personal mobile devices (see also: question 1.6.4). Template policies at cpe.org.uk/ds. For materials that help staff be aware of WiFi practices, see www.cpe.org.uk/wifi and cpe.org.uk/dstraining. Staff may have signed agreements when they joined to confirm appropriate password practices would be used. Various template documents encourage proper WiFi practices: ▪ Template 2 "Staff confidentiality agreement" ▪ Template 3A "Staff confidentiality code" ▪ Templates 14A/B "Staff signature lists"	☐
7.2.1 – How does your organisation test the data and cyber security aspects of its business continuity plan?	▪ State in the text box that "a continuity test occurred" if or once that is the case. ▪ The 'continuity' section of Template 13 ", Audit checklist for spot check incl continuity test", includes an exercise to test continuity.	Some of your annual training (see questions within section 3 for Toolkit questions about training) could include a discussion session amongst all staff and a review of relevant documents. The training may cover all staff being reminded about (1) which suppliers to contact if there is an unexpected outage of internet/power/system; (2) where the copy of the supplier's contact information is kept (accessible even if the primary digital systems fail); (3) which persons within the organisation to contact in the event of a significant incident. A business continuity template can be populated with contact information and more. See cpe.org.uk/bcp. Some example incidents to test by planning or discussing are the loss of power/internet/system or a virus attack on your clinical IT system.	☐
7.3.1 – How does your organisation ensure that there are working backups of all critical data and information?	▪ Enter "My clinical system supplier has set up backup systems" if so. ▪ Note: All EPS system suppliers have advised Community Pharmacy England that backup systems are in place. However, the options may vary even for pharmacies that use the same PMR system	Ensuring you have a process for backing up data is essential because if your systems fail or become disrupted and your access to the data is lost, this could impact the running of your pharmacy. Further Guidance can be found at cpe.org.uk/backups and within the notes of this document. Note about this technical question: this is a question that your IT system suppliers or IT support may be able	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
	with factors such as backup frequency variables depending on the contract and arrangements.	to help you answer (see FAQ at the bottom of this document). *	
7.3.2 – All emergency contacts are kept securely, in hardcopy and are up-to-date.	▪ Check the list is current, and make changes if needed. ▪ Tick and save	Locate the emergency contacts list from the business continuity plan. Find the link to this at cpe.org.uk/dstemplates.	☐
7.3.4 – Are backups routinely tested to ensure data and information can be restored?	▪ Tick and save if this is known to be the case. ▪ Note: All EPS system suppliers have advised Community Pharmacy England that backup systems are in place (see question 7.3.1).	Note about this technical question: this is a question that your IT system suppliers or IT support may be able to help you answer (see FAQ at the bottom of this document). *	☐
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?	▪ Tick and save if your IT systems are sufficiently up-to-date or there is some unsupported software, but some mitigations are in place. ▪ Most IT support or IT suppliers will provide information that says the software they provide (e.g., Windows 10 versions) are automatically updated. If so, you may review the answer.	The scope relates to clinical systems that transfer patient data, e.g., your PMR system and your IT services system. You may enter "Clinical systems are regularly updated" or "Addressed within Asset Register" if so. The "Asset Register" column and 'Software Notes' column can be used to mark critical software no longer supported – see question 8.2.1. Related guidance is available at cpe.org.uk/itupdates and cpe.org.uk/windows. Note about this technical question: this is a question that your IT system suppliers or IT support may be able to help you answer (see FAQ at the bottom of this document). *	☐
8.2.1 – If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a	▪ Enter 'N/A' if no unsupported software is used (note: the scope is limited to systems through which patient data is transferred). ▪ If Windows systems had data flowing through, you may list these internally as no longer supported (e.g., within your internal asset register) or	Also see question 8.1.1: the list of unsupported software may also be listed within the asset register (Template 6 at cpe.org.uk/dstemplates), and the Toolkit and the risk assessment information could also be detailed within the document. A risk assessment may include any plans for migrating to a newer supported equivalent software in the future, information about what information flows through the software, and the importance of access to the software.	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.	within the Toolkit. The Community Pharmacy IT Group (CP ITG) Windows 7/10 guidance can be found at cpe.org.uk/windows. It includes suggested transition plans if not completed and mitigations if any machines remained on an older Windows version for a period. ▪ Your IT support may have provided information to confirm that your software (e.g., Windows) is automatically updated. If so, you may review the information provided to assist your Toolkit answer.	Learn more about unsupported software and dealing with it at cpe.org.uk/settings. For some of your answers, you may choose to state that the information requested is within a particular document where that is the case, e.g., the Template 6 "Asset register" (at cpe.org.uk/dstemplates), rather than disclose what could be sensitive information. Note about this technical question: this is a question that your IT system suppliers or IT support may be able to help you answer (see FAQ at the bottom of this document). *	
8.3.5 - How does your organisation ensure the latest software updates are downloaded and installed?	▪ Many PMR suppliers may have provided information about their strategy for auto-updating relevant systems. If so, you may use or review the answer. EPSR2 PMR system suppliers reported to Community Pharmacy England that relevant updates are automatically rolled out where they manage systems.	Note that the scope relates to clinical systems which involve patient data, e.g., your PMR system and your services IT system. Such systems may be set to auto-update. Additional Community Pharmacy England guidance is available at cpe.org.uk/itupdates. Note about this technical question: this is a question that your IT system suppliers or IT support may be able to help you answer (see FAQ at the bottom of this document). *	☐
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?	▪ If your PMR supplier provided information to you, then use/review this information to assist with the answer. However, note that all PMR suppliers have confirmed to Community Pharmacy England that they have a process in place so that routers providing HSCN have their default passwords changed for EPS-using pharmacy teams.	If you have arranged an additional broadband connection to transfer sensitive information, consider the information at cpe.org.uk/routers, which signposts to guidance on how to change the default passwords on your internet router. A password is fundamental to ensure data protection. Default passwords are best changed when the network is first set up, especially if these are simple (e.g., password 'admin'). Your PMR supplier or someone acting for them will do this with any broadband routers they arrange for you. Note about this technical question: this is a question that your IT system suppliers or IT support may be able	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
	▪ If you also have broadband and clinical data flows through this, you may refer to the explanatory note.	to help you answer (see FAQ at the bottom of this document). *	
9.5.2 - Are all laptops, tablets, or removable devices that hold or allow encrypted access to personal data?	▪ Most pharmacy teams will not yet have a mobile device directly processing Spine-linked data. Most pharmacy teams can, therefore, enter 'N/A' for this question. ▪ The scope is limited to mobile devices directly processing patient data, e.g., mobile devices that may have been provided by a PMR supplier and linked to Spine/EPS. PMR suppliers have explained where they offer a Spine-linked mobile device with suitable encryption protection. Pharmacy team feedback that more of these devices being made available within the pharmacy would be helpful. ▪ Use of NHSmail on personal devices is permitted - see explanatory note.	Personal devices not processing patient data are not within scope. If you do not use mobile devices to access patient data, you can put "N/A as these methods of storing healthcare data are not used". Note: NHSmail can work on mobile devices; e.g., the use of NHSmail may auto-detect those with a passcode and a recently updated operating system. NHSmail may be used with the Microsoft Outlook smartphone app or within common web browser apps. Additionally, consider the information at: cpe.org.uk/NHSmail If you use a laptop through which patient data flows, you should check with your IT support that the appropriate encryption is in place. Note about this technical question: this is a question that your IT system suppliers or IT support may be able to help you answer (see FAQ at the bottom of this document). *	☐

Question-by-question guidance table 2 of 2 (covered within GDPR WB)

Toolkit question (mandatory and marked completed if GDPR WB is declared as refreshed)	**Action and explanatory notes (further mandatory questions)**	
1.1.1 – What is your organisation's Information Commissioner's Office (ICO) registration number?	Enter 'See GDPR WB' if you have refreshed it. If you have not completed the GDPR WB: ▪ Refer to the tooltip for completion.	
1.1.2 – Does your organisation have an up-to-date list of how it holds and shares different types of personal and sensitive information?	Enter 'See GDPR WB' if you have refreshed it. If you have not completed the GDPR WB, note that: ▪ You may wish to enter in the 'document location' field "*Information is within my asset register which is held within my organisation*" if this is the case. See Template 6, "Asset Register" [from cpe.org.uk/dstemplates], which includes a version with worked pharmacy examples.	
1.1.3 – Does your organisation have a privacy notice?	Enter 'See GDPR WB' if you have refreshed it. If you have not yet completed the GDPR WB, note that: ▪ Your Privacy Notice could be made available via a leaflet or a poster visible within the pharmacy and included on the pharmacy website. You should refer to GDPR WB Template G, "Tell people about your processes: the Privacy Notice", as this consists of a sample template (see cpe.org.uk/dstemplates). ▪ You may wish to enter 'This has been done in my Privacy Notice' if this is the case. The Privacy Notice should refer to patient rights.	
1.1.5 – Who has responsibility for data security and protection, and how has this responsibility been formally assigned?	Enter 'See GDPR WB' if you have refreshed it. If you have not completed the GDPR WB: ▪ Enter 'Yes' if responsibility is assigned. Information to assist you is available at cpe.org.uk/dsroles and Template 21 Assigning data security roles (cpe.org.uk/dstemplates). ▪ Note that (1) Responsibility must be assigned. (2) Responsibility may have been assigned within the Toolkit submission period or completed during a previous time and carried forward. ▪ If a new person(s) has taken up the role(s), their name(s) must be entered. ▪ If you or the person(s) with responsibility do not wish to have names listed in the Toolkit, you may want to input that 'The names of the persons are stored and known within the pharmacy organisation' instead of listing the names.	
1.3.1 – Does your organisation have up-to-date policies for data protection and	Enter 'See GDPR WB' if you have refreshed it. If you have not completed the GDPR WB, note that: ▪ Enter 'Yes' if approved policies are in place. ▪ Templates are found at cpe.org.uk/dstemplates	

Toolkit question (mandatory and marked completed if GDPR WB is declared as refreshed)	Action and explanatory notes (further mandatory questions)	
data and cyber security?	▪ Policies are not required to be changed yearly, but you should review them regularly (e.g. once every year), and if you identify a benefit from an amendment or a correction, you should make this.	
1.3.2 – Does your organisation monitor your compliance with data protection policies and regularly review the effectiveness of data handling and security controls?	Enter 'See GDPR WB' if you have refreshed it. If you have not completed the GDPR WB, note that: ▪ Enter "Yes" if this is the case". ▪ The spot checks about IG may be performed via process reviews and during training and staff discussions. If issues are identified and processes are subsequently improved or amended, you should insert further information into the answer box. Template 13, "Audit list for spot check", is available here: cpe.org.uk/dstemplates.	
1.3.7 – Does your organisation's data protection policy describe how you keep personal data safe and secure?	Enter 'See GDPR WB' if you have refreshed it. If you have not completed the GDPR WB: ▪ Refer to the "covers this with" column of the spreadsheet entitled "GDPR Workbook for Community Pharmacy" (GDPR WB) and the templates specified within.	
1.3.8 – Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing or changing a process or starting a new project involving personal data?	Enter 'See GDPR WB' if you have refreshed it. This question is covered in the Community Pharmacy England Model DPIA step-by-step process (Template M within the GDPR WB –cpe.org.uk/gdpr), which follows the ICO DPIA guidance and should be marked automatically completed.	
1.3.11 – If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your	Enter 'See GDPR WB' if you have refreshed it. ▪ Enter "staff mobile phones do not store patient identifiable data" if so. Pharmacy teams may want to use the mobile device policies and templates (see notes). ▪ Enter "Our organisation's policies cover the use of mobile devices and relevant mitigations" if this is the case (see notes). Relevant policies, guidance and templates:	

Toolkit question (mandatory and marked completed if GDPR WB is declared as refreshed)	Action and explanatory notes (further mandatory questions)	
organisation have a bring your own device policy and is there evidence of how this policy is enforced?	▪ cpe.org.uk/mobiledevices ▪ Template 8A "Portable Computer Devices Guidelines" ▪ Template 8B "Bring Your Own Device Policy and Guideline" ▪ Template 9 "Portable equipment control form" to support the maintenance of records ▪ Template 6, "Asset Register", enables logging mobile devices and their available features in the event of a loss.	
1.3.13 – Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.	Enter 'See GDPR WB' if you have refreshed it. If you have not completed the GDPR WB, note that: ▪ Enter 'Yes' if this is the case. ▪ Refer to Template 7, "Physical Security Risk Assessment" [see cpe.org.uk/dstemplates].	
1.4.1 – Does your organisation have a timetable which sets out how long you retain records for?	Enter 'See GDPR WB' if you have refreshed it. If you have not completed the GDPR WB, note that: ▪ Pharmacy record keeping and disposal procedures and information are covered in Template 4, "Data handling, record keeping and disposal procedures", and cpe.org.uk/dsdispose ▪ See the Records Management Code of Practice for Health and Social Care (transform. England.nhs.uk/information-governance/guidance/records-management-code/), which includes a pharmacy retention schedule you may adopt. This schedule outlines the recommended duration for retaining records and can assist pharmacy owners in determining when to dispose of a record. For instance, it suggests keeping records for at least a patient's lifetime plus ten years. This is because health record information may be needed again in the future for the patient's ongoing care or for other purposes even after their lifetime. If records are stored electronically, there is no requirement to keep a paper copy of the same information. Instead of simply keeping or deleting electronic records, there are alternative options such as archiving or 'hiding' them from typical system usage, if appropriate. However, it is important to perform archiving with care to safeguard the patient's interests. In certain scenarios, the pharmacy team may need to review older information when providing direct care. Additionally, the Specialist Pharmacy Service (SPS, SPS.nhs. UK) has created a comprehensive example document on record keeping specifically tailored for pharmacy teams.	
2.2.1 – Do all employment	Enter 'Within GDPR WB' if you have refreshed it. If you have not completed the GDPR WB, note that:	

Toolkit question (mandatory and marked completed if GDPR WB is declared as refreshed)	Action and explanatory notes (further mandatory questions)	
contracts and volunteer agreements contain data security requirements?	▪ Template 2, "Staff Confidentiality Agreement"[see https://cpe.org.uk/dstemplates], includes the clause that staff members will agree not to disclose during or after employment any information of a confidential nature. This clause can be used within employment contracts.	
3.1.1 – Has a training needs analysis covering data security, protection, and cyber security been completed in the last twelve months?	Enter 'Within GDPR WB' if you have refreshed it. See also: cpe.org.uk/dstraining. A pharmacy training analysis document is at: https://cpe.org.uk/dstraining: Template 3D "Training options and analysis". The organisation's 'training needs analysis' considers the pharmacy's data security and training needs and how these can be met. You can decide what level of training on data security and protection is required for staff grades or roles. You are responsible for ensuring that staff members complete this training. If you have reviewed the GDPR WB note that: There should be an assessment for all staff (this assessment confirms that every staff member has or will be re-trained with the support of one of the following recommended training options: ▪ the Template 3B "Pharmacy data security and IG training (for induction or refreshment)" (cpe.org.uk/dstrainingrefresher); ▪ "GDPR Guidance for Community Pharmacy (short version) (Part 2) staff training booklet" (see cpe.org.uk/dstraining); ▪ NHS England Data security awareness level 1 (see cpe.org.uk/dstraining); or ▪ equivalent (see cpe.org.uk/dstraining). The IG lead person(s) should undertake more detailed training, e.g., GDPR Guidance (Part 1) (see question 3.4.1, which relates to training for IG leads and cpe.org.uk/dstraining 'IG lead training' section). All staff require annual re-training (see question 3.2.1). Some staff may receive ad hoc training throughout the year, e.g., discussions or memos about good data security practices. Support organisations like Community Pharmacy England may also issue data security best practice information. It is suggested that you keep an internal record of training session dates or dates that staff confirm they have reviewed training materials. New staff should undergo a data and security training induction shortly after arrival.	
6.1.1 – Does your organisation have a system to report data breaches?	Enter 'Within GDPR WB' if you have refreshed it. If you have not completed the GDPR WB, note that: ▪ Pharmacy owners may use the Template 11, "Incident management procedures", and, where needed, Template 12 ", Incident report form (data security)" [see https://cpe.org.uk/dstemplates]. ▪ Refer to GDPR WB Template I, "Consider personal data breaches"[see https://cpe.org.uk/dstemplates] and use this to inform your process in case of future data breaches. ▪ You may consider the level of breaches in line with your process to help decide any further action required, noting that some types of violations must be reported swiftly to the relevant place, e.g., the Information Commissioner's Office (ICO).	

Toolkit question (mandatory and marked completed if GDPR WB is declared as refreshed)	Action and explanatory notes (further mandatory questions)	
	▪ You can use the 'Report an Incident' function within the DSPTK Incident reporting tool. If you do so, then dependent on your responses, the information you provide could be sent to any of the following: the Information Commissioner's Office, the Department of Health and Social Care, NHS England and NHS Improvement, and the National Cyber Security Centre.	
6.1.2 – If your organisation has had a data breach, were the management team notified, and did they approve the planned actions to minimise the recurrence risk?	Enter 'Within GDPR WB' if you have refreshed it. ▪ If the GDPR WB was not completed and there were no data breaches, then tick the box and state "No breaches". The person responsible is typically the person with IG lead responsibilities. ▪ Pharmacy owners may make use of Template 11, "Incident management procedures", and, if necessary, Template 12 ", Incident report form (data security)" [see https://cpe.org.uk/dstemplates]. ▪ Note that guidance about data breaches can be found within GDPR WB (Part 3) Template I, "Consider personal data breaches" [see cpe.org.uk/dstemplates].	☐
6.1.3 – If your organisation has had a data breach, were all individuals who were affected informed?	Enter 'Within GDPR WB' if you have refreshed it. If you have not completed the GDPR WB, note that: ▪ Pharmacy owners may make use of Template 11, "Incident management procedures", and, if necessary, Template 12 ", Incident Report Form (data security)" [see cpe.org.uk/dstemplates]. ▪ Note that guidance about data breaches can be found within GDPR WB (Part 3) Template I, "Consider personal data breaches" [see cpe.org.uk/dstemplates]. ▪ If the breach is likely to result in a risk to the rights and freedoms of a patient, the ICO should be informed of the violation. This must be done without delay and certainly no later than 72 hours after you first become aware of the breach. ▪ If the breach is likely to result in a high risk to the rights and freedoms of a patient, the patient should also be informed of the violation. This is subject to certain caveats. Read more within GDPR WB (Part 3) Template I, "Consider personal data breaches" [see cpe.org.uk/dstemplates].	☐
7.1.2 – Does your organisation have a business continuity plan that covers data and cyber security?	Enter 'Within GDPR WB' if you have refreshed it. If you have not completed the GDPR WB: ▪ Refer to https://cpe.org.uk/bcp for further information and the community pharmacy business continuity plan template. ▪ Refer to cpe.org.uk/itcontingency for additional IT contingency guidance.	☐
10.1.2 – Does your organisation have a list of its suppliers that handle personal information, the	Enter 'Within GDPR WB' if you have refreshed it. If you have not completed the GDPR WB, note that: ▪ Enter 'Yes' if this is the case. ▪ Refer to Template 22, "Suppliers list", if required [see cpe.org.uk/dstemplates].	☐

Toolkit question (mandatory and marked completed if GDPR WB is declared as refreshed)	Action and explanatory notes (further mandatory questions)	
products and services they deliver, and their contact details?		
10.2.1 – Do your organisation's IT system suppliers have cyber security certification?	Enter 'Within GDPR WB' if you have refreshed it. All the EPS suppliers have confirmed ICO registration, completion of the DSPTK annually and ISO270001 (a data security standard). Some suppliers will have additional certification even if some of this is beyond the minimum expected standard, e.g., example certification ISO9000 is a defined set of international standards on quality management and quality assurance. If you have not completed the GDPR WB, note that: ▪ Pharmacy info and template processor lists are available at https://cpe.org.uk/dataprocessors Note about this technical question: this is a question that your IT system suppliers or IT support may be able to help you answer (see FAQ within the document). *	

***Q. How can my PMR supplier help me with technical questions?**

Community Pharmacy England has been working with PMR suppliers on various matters relating to the 2024/25 Toolkit. We are aware that some PMR suppliers have plans to offer information and guidance to assist pharmacy teams in answering the 18 mandatory technical questions in different ways. This may include providing guidance documents or offering support through their helpdesk.

A few PMR suppliers may also utilise the improved Toolkit PMR feature. This feature involves your PMR supplier setting up an email address (e.g., igsupport@pmr.com) for communication purposes. You would enter this email address within the 'Admin'>'User List' section of the Toolkit as a 'Member' Your PMR supplier would then bulk-insert some information for the mandatory technical questions at a pre-set time, as advised by them. If necessary, you can add or modify the answers provided by your PMR supplier to include additional information after the bulk-insertion. As a 'Member', the PMR supplier would technically have visibility of the answers, but they must have provided a written promise not to collect, read, or review this information. However, it is advised not to rely solely on your PMR supplier using the Toolkit PMR feature if they choose not to do so this year.

Further support

For an overview of how to complete the Toolkit, you can refer to the Briefing: Toolkit overview. More information can be found at cpe.org.uk/ds, cpe.org.uk/dsfaqs and dsptoolkit.nhs.uk/help. Requests for support can also be emailed to exeter.helpdesk@nhs.net or telephone: 0300 3034034.

If you have questions about this Community Pharmacy England Briefing, please contact Daniel Ah-Thion, Community Pharmacy IT Policy Manager, it@cpe.org.uk, or Katrina Worthington, Regulations Officer.

Read Community Pharmacy England's step by step guide:

- Preparing for and using the Toolkit HQ batch feature