December 2022

PSNC Briefing DS23B: Question-by-question guidance on how to complete the Data Security and Protection Toolkit 2022/2023 (mandatory questions)

This document contains guidance for community pharmacy contractors about how to complete the mandatory questions contained in the **2022/23** Data Security and Protection Toolkit ('Toolkit').

Contractors are required to complete all questions marked mandatory within the Toolkit in order to make their annual information governance (IG) declaration.

Those contractors who have refreshed ('completed') their General Data Protection Regulation (GDPR) Workbook ('GDPR WB'), released previously, are reminded to enter "See GDPR WB" for around half of the Toolkit questions. The GDPR WB auto completion feature is not included within the 2022/23 Toolkit.

PSNC 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

For an overview of how to complete the Toolkit, read the **Briefing: Toolkit overview** which explains how to:
- login to the toolkit;
- begin updating and completing your "Organisation Profile";
- confirm that your GDPR WB has been refreshed (i.e. marked 'completed' within the organisation profile - see above), this includes ensuring the personnel sections and contract sections are refreshed;
- provide refresher training to your staff; and
- use the "batch" submission, if appropriate; contractors with three or more pharmacies may benefit from using this feature. You can find out how to use this feature by referring to: Toolkit: Using the Data Security and Protection Toolkit's POC batch submission feature: step-by-step guide. This guide explains how to request that this feature be set up for your pharmacies.
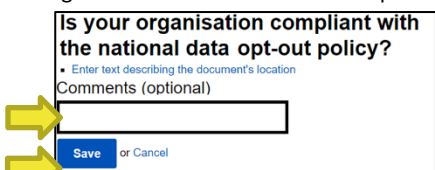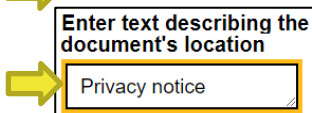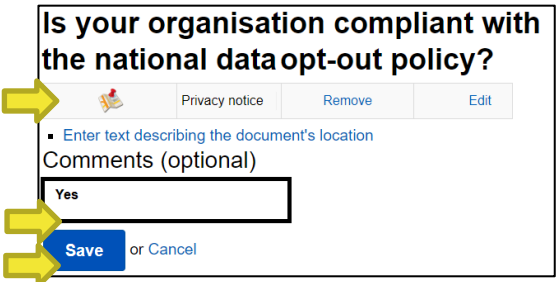
Please work your way down the outstanding Toolkit questions using the tables below. In the tables:
- Rows with a grey background signify technical questions that your IT support may be able to help answer (see final page).
- Purple questions are those that are new or have been significantly re-worded/refreshed. These questions will benefit from a more careful review.

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

Table 2 of 2 (pages 10-12) includes guidance for the other mandatory questions – for those contractors that have not completed/refreshed the GDPR WB.

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?	• Enter 'Yes' if the two following reasons apply (see also psnc.org.uk/optout which explains this issue in more detail). **1**. **Contractors should reference the opt-out policy within their own privacy notices** (which should be made available on contractors websites and/or within leaflets given to patients that request information). You should reference the opt-out system within your privacy notice: The PSNC privacy notice template (see psnc.org.uk/dstemplates Template 5) already includes 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.*". If you do not use this template, you can add this clause to the wording of your own privacy notice . A separate question in the Toolkit asks you to confirm that you have a privacy notice. **2**. **Pharmacy contractors should not need to use identifiable patient data for planning/ research purposes**. **About the opt-out system**: The opt-out system allows patients to directly express their preference as to whether health and care organisations can process their personal identifiable information. The only reason (or basis) for doing this is for *Research or planning purposes*, e.g. to find ways to improve treatments or using data to improve the delivery of health services. Patients can find out more and express their opt-out preference by: • visiting the nhs.uk/yournhsdatamatters website portal; • using the NHS App; • writing by post using the instructions at the nhs.uk website; or by • calling the NHS Digital contact centre - 0300 303	Within the Toolkit opt-out question you are also advised to click the 'enter document's location' option and type 'Privacy notice' if your notice references the opt-out. Patients have been notified about the opt-out via NHS transparency notices. The Template 5 "Privacy notice" (**psnc.org.uk/dstemplates**) includes 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.]". The below images demonstrate how you can complete the question. You can click 'save' to complete the question. You may also enter 'Yes' into the optional comments box if you align with the opt-out policy for the reasons set out within this guidance and at psnc.org.uk/optout. This **opt-out briefing** explains further how to complete this question and provides some background information about the topic. Contractors are advised to signpost patients that ask about opt-out to one of the patient-facing options on the left. PSNC and the **Community Pharmacy IT Group**, considered community pharmacy data flows in light of the opt-out system and determined that these data flows are not necessary for planning/research but that this data is processed for other reasons: I.e. legal obligations (e.g. Pharmacy Terms of Service), healthcare. Non-healthcare personal data processed for marketing purposes may relate to a basis of consent having been obtained. **PMR suppliers** and the **aggregator** companies they work with may process data for pharmacy contractors. These companies should also complete the Toolkit including the opt-out question. PMR suppliers, aggregators and others may refer to NHS Digital opt-out guidance. PSNC plans to list those PMR systems and aggregators that have confirmed compliance with the opt-out system here: **psnc.org.uk/optout**. Note: This	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
	5678 (open workdays Monday-Friday, 9am-5pm). Patients were previously informed that their opt-out preference will be honoured by health and care organisations **by 2021 or before**. NHS Digital have granted organisations an extra extension until July 31st 2022.	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 patients' 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.	
1.3.12 - How does your organisation make sure that paper records are safe when taken out of the building?	• Contractors 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 may process some limited data outside of the pharmacy when needed and appropriate. Policies and templates can support off-site processing (see notes).	• Template 3 Staff confidentiality code, Template 2 Staff confidentiality agreement and Template 1 Data security policy include passages about remote working. • Most pharmacy teams will not process patient identifiable information outside of the pharmacy. Some pharmacy teams have a policy in place outlining the precautions that must be taken when processing data outside of the pharmacy. These precautions include:: -avoiding 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 in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?	• Contractors could enter "staff mobile phones do not store patient identifiable data" if this is the case. It is recommended that contractors use the mobile device policies and templates (see notes). • Or contractors could enter "Our organisation's policies cover the use of mobile devices and relevant mitigations" 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 **pharmacy**.	Policies, guidance and templates available for contractors include: • **psnc.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 the logging of mobile devices and associated information about them.	☐
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	• 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" • **psnc.org.uk/dsdispose** • Template 22 "List of suppliers that process data"	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
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?	• Contractors should 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" • **psnc.org.uk/dsdispose** • Template 22 "List of suppliers that process data"	☐
2.1.1 - Does your organisation have an induction process that covers data security and protection, and cyber security?	• Confirm whether appropriate induction training on data security and protection is provided to all new staff. • Tick and save.	Those who have refreshed the GDPR WB should have provided refresher training to all staff. If you have not refreshed the GDPR WB this year, note that the recommended training options include: • the Template 3B "Pharmacy data security and IG training (for induction or refreshment)" (**psnc.org.uk//dstrainingrefresher**); • "GDPR Guidance for Community Pharmacy (short version) (Part 2) staff training booklet" (see **psnc.org.uk/dstraining**); • NHS Digital Data security awareness level 1 (see **psnc.org.uk/dstraining**); or • equivalent (see **psnc.org.uk/dstraining**). New joiners should sign the Template 14 staff signature list (**psnc.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.	☐
3.2.1 - Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and 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: • the Template 3B "Pharmacy data security and IG training (for induction or refreshment)" (**psnc.org.uk//dstrainingrefresher**); • "GDPR Guidance for Community Pharmacy (short version) (Part 2) staff training booklet" (see **psnc.org.uk/dstraining**); • NHS Digital Data security awareness level 1 (see **psnc.org.uk/dstraining**); or • equivalent (see **psnc.org.uk/dstraining**). Ensure that 95% or more of all current staff (including delivery drivers etc) have completed such training or equivalent. In practice for a small pharmacy, this is likely to be the entire pharmacy team.	☐
3.4.1 - Have the people with responsibility 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 as well as any other leaders and company directors have completed advanced training appropriate to their roles. Advanced training includes GDPR and data security and protection (see **psnc.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.	Contractors need to confirm that this record is maintained.	☐
4.2.4 - Does your organisation have a reliable way of	• Tick and save once you are confident about the method, and that	You may keep a list of current staff that need IT rights, using **psnc.org.uk/dstemplates:** Template 6 "Asset register" or Template 14C "List of staff and IT rights". Template 15 "Access	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
removing or amending people's access to IT systems when they leave or change roles?	only current staff have access to key IT systems.	control, passwords & accounts procedures" will assist processes within the pharmacy. Template 13 "Audit spot checks" will also assist with checking that leavers IT rights have been revoked. Additional background information: • Some information can be accessed only from within the system. • Smartcards which are not used at all become locked. • Personal NHSmail accounts which are not used for a period become deactivated.	
4.5.4 - How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?	• Tick and save if all staff are familiar with good password practice. This will have been covered in the refresher staff training question • Staff can be trained or refreshed - see Explanatory notes. • Staff may have signed agreements when they first joined to confirm they would follow appropriate password practice.	For materials that inform staff about good password practices, see **psnc.org.uk/passwords** and **psnc.org.uk/dstraining**. The following template documents (**psnc.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" • 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?	• If there have been no security breaches, then insert "N/A" in the free text box. • 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 issues that were identified and how the process has been improved to reduce the likelihood of reoccurrence. • Click save	A review of data security problems including near misses or breaches should be carried out at least once a year. Pharmacy contractors are advised to use the following resources when conducting such a review: Template 11 "Incident management procedures" and where needed, Template 12 "Incident report form (data security)" (which are both available at **psnc.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 Digital can pass on information required including 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 numbers of data subject, 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 not possible to provide immediately, should be provided later without undue delay. A review of processes may be appropriate after any data breach or near miss in case adjustments can be made to people and/or 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 is included the pharmacy devices that are used to process patient data.	Antivirus protection is essential to protect the pharmacy system from viruses that can compromise data. If you are unsure about what anti-virus software is used, then check this or contact your IT support. Note that some devices may come with pre-installed antivirus software. Additional guidance is available at: **psnc.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 PMR pharmacy system supplier 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 use of public Wi-Fi for work purposes is unsafe?	• Tick and save if all staff are aware that access to sensitive work data over a public WiFi network is not appropriate (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 contractors 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 **psnc.org.uk/ds**. For materials that help staff to be aware about WiFi practices, see **www.psnc.org.uk/wifi** and **psnc.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?	• Contractors could 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 also include a discussion session amongst all staff and/or 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 main digital systems fail); (3) which persons within the organisation to contact in the event of a major incident. A business continuity template can be populated with contact information and more. See **psnc.org.uk/bcp**. Here are some example incidents to test by planning or discussing: the loss of power/internet/system; a virus attack on the PMR system.	☐
7.3.1 - How does your organisation make sure that there are working backups of all important data and information?	• Contractors should enter that "My clinical system supplier has set-up backup systems" if this is the case. • Note: All EPS system suppliers have advised PSNC that backup systems are in place. However, the options may vary even for pharmacies which use the same PMR system with factors such as backup frequency variable depending on the contract and arrangements in place.	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 **psnc.org.uk/backups** and within the notes of this document. Note about this technical question: this is a question that your PMR pharmacy system supplier or IT support may be able 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 list is up to date and make changes if needed. • Tick and save	Locate emergency contacts list from business continuity plan. Find the link to this at **psnc.org.uk/dstemplates**.	☐
7.3.4 - Are backups routinely tested to make sure that data and information can be restored?	• Tick and save if this is known to be the case. • Note: All EPS system suppliers have advised PSNC that backup systems are in place (see question 7.3.1).	Note about this technical question: this is a question that your PMR pharmacy system supplier 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	• Tick and save if your IT systems are sufficiently up-to-date or there is some unsupported software, but some mitigations are in place.	The scope relates to clinical systems used for the transfer of patient data e.g., your PMR system and PharmOutcomes. You may choose to enter "Clinical systems are regularly updated" or "Addressed within Asset Register" if this is the case. The "Asset	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
manufacturer or the risks are understood and managed?	• Most IT support or PMR suppliers will provide information to say that your PMR software and the software they provide (e.g., Windows 10 versions) is automatically updated. If so, you may review the answer.	Register" column 'Software Notes' column can be used to mark critical software no longer supported – see question 8.2.1. Related guidance is available at **psnc.org.uk/itupdates** and **psnc.org.uk/windows**. Note about this technical question: this is a question that your PMR pharmacy system supplier 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 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.	• Enter 'N/A' if there are no unsupported software 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 if no longer supported (e.g., within your internal asset register) or within the Toolkit. The Community Pharmacy IT Group (CP ITG) Windows 7/10 guidance can be found at **psnc.org.uk/windows** which includes suggested transition plans if not completed, as well as mitigations if any machines remained on an older Windows version for a period. • Your IT support may have provided information to you to confirm that your PMR software and the software they provide (e.g., Windows) is automatically updated. If so, you may review the information provided to assist your Toolkit answer.	Also see question 8.1.1: the list of unsupported software may also be listed within the asset register (Template 6 at **psnc.org.uk/dstemplates**) and/or within the Toolkit, and the risk assessment information could also be listed 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 is flowing through the software; the importance of access to the software. Learn more about unsupported software and dealing with it at **psnc.org.uk/settings**. For some of your answers you may choose to state that the information requested is within a certain document where that is the case e.g., the Template 6 "Asset register" (at **psnc.org.uk/dstemplates**), rather than disclose what could be sensitive information. Note about this technical question: this is a question that your PMR pharmacy system supplier 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 make sure that the latest software updates are downloaded and installed?	• Many PMR suppliers may have provided information about their strategy for the auto-updating of relevant systems. If so, you may use or review the answer. EPSR2 PMR system suppliers reported to PSNC that where they manage systems, relevant updates are automatically rolled out.	Note that the scope relates to clinical systems which involve patient data e.g., your PMR system and PharmOutcomes. Such systems may be set to auto-update . Additional PSNC guidance is available at **psnc.org.uk/itupdates**. Note about this technical question: this is a question that your PMR pharmacy system supplier 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 the answer. However, note that: all PMR suppliers have confirmed to PSNC that they have a process in place so that routers providing N3/HSCN have their default passwords changed for EPS-using pharmacy contractors. • If you also have your own broadband and clinical data flows through this, you may refer to explanatory note.	If you have arranged an additional broadband connection used for transfer of sensitive information then consider the information at **psnc.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 which they arrange for you.	☐

Toolkit question (mandatory and not covered by GDPR WB)	Action	Explanatory notes	
		Note about this technical question: this is a question that your PMR pharmacy system supplier or IT support may be able to help you answer (see FAQ at the bottom of this document).*	
9.5.2 - Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	• Most contractors will not yet have a mobile device that is directly processing any Spine-linked data. Most contractors will therefore be able to 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 provide a Spine-linked mobile device suitable encryption protection is in place. Pharmacy team feedback continues to be 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 then you can put "N/A as these methods of storing healthcare data are not used". Note: That NHSmail can work on mobile devices, e.g., 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: **psnc.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 PMR pharmacy system supplier 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 tool tip for completion.	☐
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?	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 **psnc.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 that is visible within the pharmacy and/or included on the pharmacy website. It is recommended that you refer to GDPR WB Template G "Tell people about your processes: the Privacy Notice" as this includes a sample template (see **psnc.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	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 **psnc.org.uk/dsroles** and Template 21 Assigning data security roles (**psnc.org.uk/dstemplates**).	☐

Toolkit question (mandatory and marked completed if GDPR WB is declared as refreshed)	Action and explanatory notes (further mandatory questions)	
responsibility been formally assigned?	• Note that: (1) Responsibility must be assigned. (2) Responsibility may have been assigned within the Toolkit submission period or may have been completed during a previous time and carried forward. • If 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 wish to input that 'The names of the persons are stored and known within the pharmacy organisation' as opposed to listing the names.	
1.3.1 - Does your organisation have up to date policies in place for data protection and for data and cyber security?	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 **psnc.org.uk/dstemplates** • 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 own 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 in relation to IG may be performed via process reviews and / or 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: **psnc.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 PSNC Model DPIA step-by-step process (Template M within the GDPR WB - **psnc.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 organisation have a bring your own device policy and is there evidence of how this policy is enforced?	Enter 'See GDPR WB' if you have refreshed it. • Contractors should enter "staff mobile phones do not store patient identifiable data" if this is the case. Pharmacy contractors 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 : • **psnc.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 maintenance of records • Template 6 "Asset Register" enables the logging of mobile devices and their available features in the event of loss.	☐
1.3.13 - Briefly describe the physical controls your buildings have that prevent	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 **psnc.org.uk/dstemplates**].	☐

Toolkit question (mandatory and marked completed if GDPR WB is declared as refreshed)	Action and explanatory notes (further mandatory questions)	
unauthorised access to personal data.		
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 **psnc.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 that you may adopt. This schedule sets out how long records should be retained and will help contractors to decide when to dispose of a record. For example: suggestions include records being kept for at least the life of a patient plus 10 years. Health record information may be required again later for the patient's care within their lifetime or for another purpose after their lifetime. 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 patients' 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.	☐
2.2.1 - Do all employment contracts, and volunteer agreements, contain data security requirements?	Enter 'Within GDPR WB' if you have refreshed it. If you have not completed the GDPR WB note that: • Template 2 "Staff Confidentiality Agreement"[see https://psnc.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 and protection, and cyber security, been completed in the last twelve months?	• Enter 'Within GDPR WB' if you have refreshed it See also: **psnc.org.uk/dstraining** A pharmacy training analysis document is at: https://psnc.org.uk/dstraining: Template 3D "Training options and analysis". The organisations 'training needs analysis' considers the data security and training needs of the pharmacy 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 and are responsible for ensuring that staff members complete this training. Contractors that have reviewed the GDPR WB should have completed 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)" (**psnc.org.uk/dstrainingrefresher**); • "GDPR Guidance for Community Pharmacy (short version) (Part 2) staff training booklet" (see **psnc.org.uk/dstraining**); • NHS Digital Data security awareness level 1 (see **psnc.org.uk/dstraining**); or • equivalent (see **psnc.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 **psnc.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 across the year e.g., discussion or memos issued to staff about good data security practices. Support organisations such as PSNC may also issue good data security practice information across the year. 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 their arrival	☐
6.1.1 - Does your organisation have a system in place to report data breaches?	Enter 'Within GDPR WB' if you have refreshed it If you have not completed the GDPR WB note that: • Pharmacy contractors may make use of: Template 11 "Incident management procedures" and, where needed, Template 12 "Incident report form (data security)" [see https://psnc.org.uk/dstemplates].	☐

Toolkit question (mandatory and marked completed if GDPR WB is declared as refreshed)	Action and explanatory notes (further mandatory questions)	
	• Refer to GDPR WB Template I, "Consider personal data breaches"[see https://psnc.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 breaches must be reported swiftly to the relevant place e.g. Information Commissioner's Office (ICO). • You have the option to 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 actions planned to minimise the risk of a recurrence?	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 contractors may make use of: Template 11 "Incident management procedures" and, if necessary, Template 12 "Incident report form (data security)" [see https://psnc.org.uk/dstemplates]. • Note that guidance about data breaches can be found within GDPR WB (Part 3) Template I "Consider personal data breaches" [see **psnc.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 contractors may make use of Template 11, "Incident management procedures" and, if necessary, Template 12 "Incident report form (data security)" [see **psnc.org.uk/dstemplates**]. • Note that guidance about data breaches can be found within GDPR WB (Part 3) Template I "Consider personal data breaches" [see **psnc.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 breach. 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 breach. This is subject to certain caveats. Read more within GDPR WB (Part 3) Template I "Consider personal data breaches" [see **psnc.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://psnc.org.uk/bcp for further information and the community pharmacy business continuity plan template. • Refer to **psnc.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 products and services they deliver, and their contact details?	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 **psnc.org.uk/dstemplates**].	☐
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://psnc.org.uk/dataprocessors Note about this technical question: this is a question that your PMR pharmacy system supplier or IT support may be able to help you answer, (see FAQ within the document).*	☐

*Q. How might my PMR supplier assist me with the technical questions?

PSNC has been working with PMR suppliers on various matters relating to the 2022/23 Toolkit. We are aware that some PMR suppliers are planning to provide information and guidance to support contractors' completion of up to 18 technical mandatory questions in a variety of ways, e.g., via guidance documents or their helpdesk.

A few PMR suppliers may utilise the improved **Toolkit PMR feature**. This feature involves your PMR supplier setting up an email address (e.g., igsupport@pmr.com) to be communicated to you and entered by you (within the 'Admin'>'User List' section of the Toolkit, as a 'Member') so that some information can be inserted in bulk for the mandatory technical questions. This is likely to be at a pre-set time about which your PMR supplier would advise you. You will be able to add or amend the answers entered by your PMR supplier to include more information after the final bulk-insertion, if necessary. As a 'Member', the PMR supplier would technically have visibility of answers but would need to have promised in writing not to collect, read, or review these. You are advised not to wait for your PMR supplier to use the Toolkit PMR feature in case they choose not to use the feature this year.

Further support

For an overview of how to complete the Toolkit read: **Briefing: Toolkit overview**.

More information can be found at: **psnc.org.uk/ds**, **psnc.org.uk/dsfaqs** and **dsptoolkit.nhs.uk/help**. Requests for support can also be made by email to **exeter.helpdesk@nhs.net** or telephone: 0300 3034034.

If you have any questions or concerns about this Briefing, please contact **Daniel Ah-Thion**, PSNC's Community Pharmacy IT Policy Manager.