Data and Security Protection (IG) toolkit technical questions

(Mandatory)

Ref and change	QUESTION	QUESTION TIP	Question answer might be covered off by pharmacy GDPR workbook (pharmacy doesn't re-answer if done workbook)	PSL - Text for managed and non-managed customers from PMR supplier (draft) – example template text	General tips (many applicable to pharmacy) or info for PMR template answer
1.4.4	Is your organisation compliant with the national data opt-out policy?	The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic. As a provider, you should help the people who use your services to understand that they can opt out of their data being used for other purposes. You should check that your policies, procedures, and privacy notice cover the opt out. All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 31 March 2021. If you are not CQC registered the below link gives advice. More detailed guidance that gives advice about compliance with the national data opt-out policy is available		**Patient identifiable data does not leave the Analyst system and is only stored within the local system for the purpose of providing Healthcare services.**	• Pharmacy contractors and their data handlers (e.g. PMR suppliers) have reported at CP ITG meetings during 2018 that using personal data has not needed the research/planning as main basis given other reasonings: e.g. legal obligations, healthcare, or for non-healthcare personal data information processing consent may be obtained. See also: https://psnc.org.uk/optout

		from NHS Digital and Digital Social Care..			
4.2.5 NEW	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people's access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box		**Analyst controls assistant permissions which can be monitored locally. Head Office or the IG lead within your pharmacy can control the assistant template using a system called Product Modeller. Each assistant's permission is viewable within the assistant details screen"**	Some systems (e.g. PMR systems or other systems) will include: (1) user lists within the system itself that you can access; and/or lists that are accessible by the system supplier; and (2) auditability for monitoring or analysis of usage by different users
6.2.3 CHG	Do all the computers and other devices used across your organisation have antivirus/antimal ware software which is kept up to date?	This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or other devices, then tick and write "Not applicable" in the comments box. Further information is available from Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/have-up-to-date-antivirus-software/ and pharmacy info at psnc.org.uk/antivirus.		**All PCs supplied by PSL for the use of processing electronic prescriptions are installed with ESET Endpoint Antivirus. Each instance is set to automatically scan and update regularly to better prevent risks from new threats.**	Antivirus protection is essential to protect the pharmacy system from viruses which can compromise data. If you are unsure about what anti-virus is used then check this or contact your IT support. Note that some devices may come with pre-installed antivirus e.g. Apple devices may include in-built software. Additional guidance is at: psnc.org.uk/antivirus
7.3.1 NEW	How does your organisation make sure that there are working backups of all important data and information?	It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation's backup systems work and how you have tested them. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any		**The Analyst system can be backed up to a separate storage device (usually a USB memory stick) and additionally in many cases to a 3rd party cloud-based solution. Data backed up to the cloud based solution is monitored by PSL support staff to ensure it is no more**	

		computers or IT systems, write “Not applicable” in the text box. For advice about backups, see Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-myinformation/cyber-security/back-up-your-data/ and pharmacy info at https://psnc.org.uk/backups		**than 3 days since the last backup.**	
7.3.4 NEW	Are backups routinely tested to make sure that data and information can be restored?	It is important that your organisation’s backups are tested at least annually to make sure data and information can be restored (in the event of equipment breakdown for example). You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, then tick and write “Not applicable” in the comments box.		**PSL do not recommend attempting to restore backups without the assistance of the PSL service desk as this may inadvertently lead to Overwriting live data with a backup. PSL regularly tests the restore process in their backup environments.**	
8.1.4 CHG	Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?	Systems and software that are no longer supported by the manufacturer can be unsafe as they are no longer being updated to protect against viruses for example. You may need to ask your IT supplier to assist with answering this question. Examples of unsupported software include: Windows XP, Windows Vista, Windows 7, Java or Windows Server 2008. Windows 8.1 is supported until January 2023. Windows 10 is supported and is the most up to date version of Windows. This question also applies to software systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems or software, then tick and write “Not applicable” in the comments box. For guidance (including information on how to check which software versions you have), see Digital Social Care. https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-		**PSL supplied hardware runs Windows 10 operating systems which still receive free security updates from Microsoft. or where a site continues to use Windows 7 operating system the option to purchase extended support updates has been provided.**	Pharmacy guidance: Related guidance is at psnc.org.uk/itupdates and psnc.org.uk/windows.

		latest-software-updates/ And pharmacy info at psnc.org.uk/itupdates			
8.2.1 CHG	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.	This is a conscious decision to accept and manage the associated risks of unsupported systems. This document should indicate that your board or management team have formally considered the risks of continuing to use unsupported items and have concluded that the risks are acceptable. If your answer to the previous question was yes, write "Not applicable" in "Enter text describing document location".		**PSL: "Analyst PMR operates on Windows 7 or higher. The PMR software is supported and regularly updated~~,~~ All Systems running Windows 10 will automatically download Microsoft updates and any sites running Windows 7 having purchased the extended life support will also receive updates.**	CP ITG (pharmacy bodies + PMRs) has updated pharmacy Windows 7/10 guidance in 2021. In pharmacy 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.
8.3.5	How does your organisation make sure that the latest software updates are downloaded and installed?	It is important that your organisation's IT system(s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any IT systems, devices or software, write "Not applicable" in the text box. Further information is available from Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/ and pharmacy info at: www.psnc.org.uk/itupdates		**PSL applications are updated automatically according to our development roadmap. The Analyst PMR system is generally updated by 2 or 3 general release versions per year. The deployment or these is managed and monitored by the PSL service team.**	Note that the scope relates to clinical systems which involve patient data

9.1.1	All networking components have had their default passwords changed	Networking components include routers, switches, hubs and firewalls at all of your organisation's locations. Your organisation may just have a Wi-Fi router. This does not apply to Wi-Fi routers for people working from home. You may need to ask your IT supplier to assist with answering this question. If your organisation does not have a network or internet access, then tick and write "Not applicable" in the comments box.		**PSL: "All network components provided by PSL have had their default passwords changed at installation. Each user of Analyst PMR manages their own log on and system password. Network device i.e. routers connected to the N3 /HSCN are managed by the appropriate internet service producer i.e. IQVIA/Redcentric. We do not necessarily support all network components. Contractors should ensure they or their supplier have updated components where these are not PSL-related e.g. by use of guidance at www.psnc.org.uk/routers."**	Example PMR answer if applies: PMR: •We have process so that every router used for EPS has its default password changed All EPS suppliers previously advised this is the process for each pharmacy customer
9.6.2 reword	Confirm all health and care data is encrypted at rest on all mobile devices and removeable media.	Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people). Devices can be further protected, for example, by preventing the use of removable devices like memory sticks. This is called computer port control. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the comments box. For advice on encrypting mobile devices and equivalent security arrangements, see Digital Social Care. https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/protect-mobile-devices-and-tablets/ and		**Data is stored within Analyst databases, either in a JET or SQL Server database. Some auxiliary data is also stored in a SQLite database. Any backups that are made are encrypted at AES256 encryption. The drives that are installed in the supplied machines are encrypted using Bitlocker.** **The JET database is protected with a password. SQL server databases are accessed using the Analyst logon and requires a strong password.**	NHSmail has protections when app or browser used. If the pharmacy uses mobile devices and/or removeable media such as a USB disk, laptop or work phone, to store patient data flows then you should ensure that these devices are encrypted. Personal devices not processing patient data are not within scope. If you don't use mobile devices to access patient data then, you can put "N/A as these methods of storing healthcare data are not used"

		pharmacy info at psnc.org.uk/mobiledevices.			

END.