

**INFORMATION GOVERNANCE QUESTIONS 2022 -23**

Section	Question 1	Question 2	Question 3	Question 4	Question 5	Question 6
<b>Introduction</b>	Background: Community Pharmacies process large amounts of information which is personal, sensitive and confidential, therefore it is crucial that adequate controls are in place. The aim of this toolkit is to provide Community Pharmacies in Wales with a list of the minimum requirements they need to adhere to.	Please supply your address below	Please confirm your PMR system supplier from the list below: Boots VCare Cegedigm Celesio Clanwilliam EMIS Health Invatech Mayberry (MBBM) Mckesson Positive Solutions Apotec	Please select your HB area: (list of HB will show below)	Completed by: Title/First name/ Last name	Date: dd/mm/yyyy
<b>Information and IT Security</b>	Does the Pharmacy premises have a named Lead for Information Governance and IT Security	Do all pharmacy staff undertake IG refresher training, at least every 2 years?	Does the Pharmacy premises have a named Caldicott Guardian Lead?	Does the Pharmacy premises have a documented Information Governance and IT Security Policy that is regularly reviewed?	Have all Pharmacy staff and locums signed a confidentiality agreement, either as part of their employment, or as a separate undertaking?	

<p><b>General Management</b></p>	<p>Do all Pharmacy staff including locums with access to Person Identifiable Information have an understanding of the principles detailed within the Information Governance and IT Security Policy, and are notified when any updates are made to it?</p>	<p>Does the Lead for Information Governance and IT Security ensure that when a staff member (including locum staff) leaves employment at the Pharmacy, that Information Governance, IT Security and confidentiality are maintained?</p>	<p>Does the Pharmacy have a process in place to notify DHCW when staff leave the Pharmacy, which includes revoking access to shared working areas? For example, NHS e-mail, Microsoft Teams work areas, etc.</p>			
<p><b>Asset Classification &amp; Control</b></p>	<p>Does the Pharmacy have a documented Assets Register encompassing software and hardware?</p>	<p>Does the Pharmacy premises have an up to date, documented Information Assets Register? (i.e. detailing; what type of information is held, where it is located and the format in which it is kept e.g. hard copy or electronically)</p>	<p>Does the Pharmacy document and maintain a record of its data processing activities?</p>			
<p><b>Data Protection &amp; Caldicott</b></p>	<p>Are Data Protection and Confidentiality addressed either in a documented policy or by their incorporation in an Information Governance and IT Security Policy?</p>	<p>Is Information Security addressed either in a documented policy or by its incorporation in an Information Governance and IT Security Policy?</p>	<p>Does the Pharmacy premises have a method of informing patients and service users about the ways in which their information will, or may be used (Privacy Information)?</p>			

<b>Freedom of Information</b>	Does the Pharmacy premises have a procedure for recording and responding to Freedom of Information (FOI) requests?	Has the pharmacy adopted an ICO model publication scheme in line with the Freedom of Information Act? (Link to ICO Website on Publication Schemes)	Is the Pharmacy Publication Scheme reviewed annually?	Does the Pharmacy have a Records Management Policy that is regularly reviewed?		
<b>IT Communications &amp; Equipment</b>	Does the Pharmacy premises have a documented procedure for disposal of IT equipment containing Person Identifiable Information to ensure confidentiality is maintained?	Does the Pharmacy have a method of ensuring that IT faults are dealt with ensuring that patients confidentiality is maintained?				
<b>Systems Management</b>	Is the Pharmacy aware of the requirements of the NHS Wales Acceptable Use Policy for use of NHS Wales provided services?	Is anti virus software present and enabled on all PC's owned by the Pharmacy operation?	Are appropriate controls in place to manage access to all computer-based information systems within the Pharmacy premises, including processes for access removal when staff leave?	Does the Pharmacy premises have a documented procedure for backing up Person Identifiable Information?	Does the Pharmacy premises comply with IT security requirements for accessing patient systems and services developed and hosted by NHS Wales?	Can your Pharmacy connect to the secure NHS IT platform to access applications such as Choose Pharmacy?

<p><b>Physical and Environmental Security</b></p>	<p>Does the Pharmacy premises have physical methods of ensuring that all Information and IT systems are secure?</p>	<p>Does the Pharmacy premises have a procedures for the secure transfer of Person Identifiable Information?</p>	<p>Does the Pharmacy have an up to date documented procedure for offsite working, whilst using electronic or hard copy Person Identifiable Information?</p>	<p>Does the Pharmacy undertake an IG risk assessment for staff including locums when working offsite from the Pharmacy premises for Person Identifiable Information?</p>		
<p><b>Incident Management</b></p>	<p>Does the Pharmacy have a documented Incident Reporting Procedure for reporting Information Governance or IT Security related incidents to the Lead for Information Governance and IT Security, the Pharmacy DPO and ICO?</p>	<p>Does the Pharmacy have a method of recording and learning from Information Governance and IT Security related incidents?</p>				

<b>Business Continuity</b>	Does the Pharmacy premises have a Business Continuity Plan for Person Identifiable Information (which includes loss of access to paper records, and the Patient Medication Records System)?	Have all relevant staff members including locum staff been made aware of this plan, its location, and their individual roles contained within it?				
--------------------------------	---	---	--	--	--	--