Update to the GDPR Workbook for Community Pharmacy

The GDPR Workbook is for the community pharmacy contractor and each community pharmacy and if completed will assist you with compliance with the GDPR and the Data Protection Act 2018 (currently draft). It will also contribute significantly to your compliance with IG requirements required by the new IG (Data Security and Protection) Toolkit that you will complete later in the year. PSNC is currently working with NHS Digital to map this across to the new Toolkit and it covers virtually all the Toolkit's essential (critical) requirements that you must achieve.

Template A: Appointing a Data Protection Officer (DPO)

To meet the DPO requirement, contractors can either appoint a member of staff or an external person, perhaps shared with other community pharmacies locally. The Community Pharmacy GDPR Working Party will issue further guidance, as will the NPA, which has agreed to lead on the issue for its members. For now, contractors should consider the following details provided by the Information Commissioner's Office (ICO):

- DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases, several organisations can appoint a single DPO between them.
- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.

Further guidance on the role of the DPO is available from the ICO and NHS Digital's Information Governance Alliance (IGA).

The DPO may be a pharmacist or another suitable person with knowledge of the particular community pharmacy and 'expert' knowledge of data protection and the GDPR and associated legislation, as this relates to that community pharmacy (for example, has a thorough understanding of the guidance issued by the Community Pharmacy GDPR Working Party, as well as the ICO and IGA guidance on the role of the DPO). The DPO is primarily an advisory role, although the DPO's name is stated on the Privacy Notice and, therefore, may be the first person to be contacted by patients or others about data protection issues and data subject rights. The DPO must not be a person who decides the purposes and means of processing, the person who decides the operational issues on data flows.

The message from those involved with GDPR is that they are not expecting everybody to be fully compliant with GDPR on 25th May 2018, not least because the UK legislation is not yet in place.

Template A: Decide who is responsible – the Caldicott Guardian

It is not mandatory for pharmacy contractors to appoint a registered Caldicott Guardian, though they may choose to do so if this makes sense for their organisation. There should be somebody at a high level within the organisation – which might be the IG Lead – who takes responsibility for protecting the confidentiality of service users' health and care data and making sure that it is used appropriately.

The Caldicott Guardian manual can be a useful resource to assist in this job role and the Caldicott Guardian Council can provide help and guidance.

Templates C

Don't forget to note which pharmacist is responsible for processing of personal data (for the contractor). This is separate to the DPO requirement. It should **not** be the DPO.

Templates I and J Data breaches

As a rough guide, because each data breach must be considered against its own facts:

1 **For any personal data breach** - record all data breaches however minor (and learn from them). E.g. if you send a patient's health data to the wrong GP or similar controlled environment where confidentiality can be assured as part of professional requirements; or if a patient's dispensed medicine has another patient's repeat slip but the error is corrected quickly in the pharmacy or soon afterwards (subject always to the circumstances and not, for example, if particularly sensitive patient data has been disclosed to somebody who knows the patient).

2 **When the data breach is 'likely to result in a risk to the rights and freedoms of the patient or other data subject'** - record the data breach and notify the ICO. What needs to be reported may change over time. Everybody will probably be cautious at the start and over report data breaches, the real danger here being that the ICO becomes overloaded with information and misses the serious problems.
E.g. if the prescription bundle is lost on route to the NHS Business Services Authority (NHS BSA) and it is not thought to be lost in the courier's warehouse.

3 **When the data breach is a high risk to the rights and freedoms of the patient or other data subject** - record the data breach, notify the ICO and tell the patient or other data subject (although as pharmacists are subject to a duty of candour, they may decide to tell the patient about something before this stage).
E.g. if a prescription collected at the GP practice has been lost on the way back to the pharmacy and could be picked up by anybody locally.

Template M: Data Protection Impact Assessment (DPIA)

Community pharmacies processing data concerning health on a large-scale must carry out a Data Protection Impact Assessment (DPIA). The Workbook made this clear. However, what is not clear is the interpretation of "large-scale". We were expecting this to be clarified as part of the discussions on the DPO issue but it has not been. Therefore, we recommend that all contractors, including smaller community pharmacies, complete a DPIA as part of preparations for GDPR compliance.

A model DPIA has been made available as an addition to the Workbook.