Findings from ICO work relating to Community Pharmacies

February 2017

Executive Summary

The Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the Data Protection Act 1998 (the DPA) and for promoting good practice in information handling. The Act consists of eight principles of good information handling that all organisations processing personal data have to comply with.

During 2016, the ICO Good Practice department undertook a series of voluntary visits with organisations operating community pharmacies in England, Scotland and Wales. In addition, the ICO also ran a survey asking community pharmacists to provide information. The scope of these visits and research focussed on the technical and organisational measures in place to address the following key issues:

- Governance around confidentiality and information security by organisations.
- Data protection issues in websites aimed at the public.
- Staff training and awareness, including refresher training and provision of data protection policies.
- Fair processing provided to customers.
- Security of personal data processed both physically and digitally.
- Records management, including retention schedules and disposal of data.
- The use of portable media devices.
- Data sharing and the transmission of personal and sensitive personal data.

The objective was to understand how these organisations are processing personal data across the UK. This report is aimed at providing feedback to the whole Community Pharmacy sector.

The outcomes of our study varied across the member organisations that took part; however the following key themes were identified that generally:

- Staff and organisations have a good awareness of the requirement to keep personal data safe and confidential and are motivated to do so.
- Organisations with multiple branches have processes in place to monitor them for compliance so maintaining standards.
- Organisational policies and procedures are widely available for staff to learn from and refer to.
- Regular training is acknowledged as an important part of the modern pharmacy setting.
- The physical layout of branches is well considered to maximise confidentiality and security.

- Confidential waste is recognised as important and disposed of securely.
- Fair processing information is available to customers in a variety of forms both either in branches or on line.

The main area of concern was that it was rare for an organisation to be consistently successful in all the areas looked at. Ongoing training was one of the hardest to execute successfully in smaller settings where resources may be more limited. Another issue was that fair processing notices on pharmacy websites often only dealt with how that website uses information, rather than how the organisation as a whole uses it.

Other areas where we would make recommendations for improvement include:

- Upgrading all computers that are processing sensitive personal data and are connected to a network to a supported operating system.
- Ensuring there is a mechanism such as “Safe Haven” procedures in place to maximise the secure use of fax machines where there are no other alternatives and their use remains necessary.
- Implementing individual user logons for all systems that contain patient identifiable data to enable a full audit trail of view and change events to a customer record.
- Eliminating the practice of shared use of NHS Smart Cards. All cards should only be used by the registered holder and systems activity audited solely to them alone.
- Ensuring that a procedure is in place to control the removal of personal data from pharmacy premises.

With the expansion of services being offered by the community pharmacy sector it is important that the basics are successfully implemented to provide a strong platform for growth and expansion.

Contents

This report covers the following:

- Our approach to working with community pharmacy organisations to produce this outcomes report.
- The types of personal information processed by organisations within community pharmacies and the issues to consider in order to comply with the DPA.
- Areas of good practice that were seen or demonstrated during our study.
- Findings and recommendations.

Approach

A review was conducted of all the cases, concerns, complaints and reported breaches of the DPA raised with the ICO relating to community pharmacies over the last three years. This was to identify trends and common areas of concern.

The ICO approached the General Pharmaceutical Council, National Pharmacy Association, Pharmacy Voice, Community Pharmacy Scotland, Community Pharmacy Wales, and the Pharmaceutical Society of Northern Ireland for assistance in working with the sector.

An online questionnaire aimed at staff working within community pharmacies was created and publicised with the help of the General Pharmaceutical Council. This was run over two months in August and September 2016 receiving 41 anonymous responses.

Assistance from the above organisations was also sought in seeking volunteers to receive fact finding visits to a range of community pharmacies. These would range from single site independents through to large multiple site national chains. This was successful and enabled 10 visits to be undertaken to sites in England, Scotland and Wales.

This report explains the areas where community pharmacies appear to be performing well, as well as highlighting the common problems and areas for improvement that other organisations can learn from. The report includes further guidance and advice to help organisations improve their data protection practices.

Unfortunately it was not possible to extend the project to include Northern Ireland or supermarket pharmacy chains; however it is likely that many of the findings are applicable in these areas.

Typical processing of personal data by community pharmacies

Community pharmacies and their staff process a significant amount of highly sensitive personal data. The nature of the business means that customers are likely to be local to the pharmacy they attend and possibly seen or known by staff outside of work.

Information held is traditionally related to drugs prescribed to a customer, however with the recent expansion in services offered by community pharmacies larger volumes of more detailed information are being recorded and held.

While the PMR will generally hold the greatest amount of patient identifiable data, physical paperwork is also kept in branch for filing that contains information.

The computer systems used in the community pharmacy setting may be wholly based on-site or may form part of an extensive networked solution.

Requests for information may be received from the police or other authorities. There may often be a friend, relative or guardian involved in a patient's care that is relevant to the work of the pharmacy and requires the sharing of information. Customers may be in residential care homes and information passed between the organisations to support patient care.

Areas of good practice

During this project many examples of good practice were seen including:

- ✓ That staff working in community pharmacies generally have a good awareness of the requirements around confidentiality and security of personal data. There seems to be a very positive attitude amongst organisations and staff to complying with the requirements of the DPA.
- ✓ There is widespread provision of training and annual refresher training on confidentiality and information security within the sector. Some organisations provided extensive role specific tailored training that is monitored and kept up to date.
- ✓ There is a widespread provision of privacy / fair processing notices or information leaflets in branch for customers.

✓ Many of the businesses with multiple locations operate a program of regular visits where as part of other work the branch's compliance with DP/IG procedures is checked. There was also often a regional or head office contact that could be asked about any DP queries.

✓ Physical layouts of Community pharmacies have been carefully thought through to maximise confidentiality and security of the information processed.

✓ Good records management takes place in branches, and currently the level of manual records does not seem to be an issue in sometimes limited retail space.

Main findings and recommendations

As a result of the ICO's study, the following themes and areas were identified. Where there are opportunities for improvement, recommendations are included.

→ WEBPAGES

Findings:
The organisations visited all had a website available online. These were split into several distinct types:

- A basic informative website, with little interactive aspects and no e-commerce. It may include a branch finder.
- A basic interactive website with the ability to create accounts and carry out non-medical e-commerce transactions. It may include the ability to request and manage repeat prescriptions.
- A fully interactive website covering all aspects of Community Pharmacy activity digitally.

The websites examined had:

- Cookie control notification in place as required by the Privacy and Electronic Communications Regulations.
- A link to the company privacy statement easily accessible.
- A link to the required FOI Publication scheme for pharmacies, (where required in England and Wales).

Some had additional welcome aspects such as:

- They set out the name and use of each cookie downloaded by the site.
- A range of information leaflets available for download.

In relation to collecting consent to be used for marketing some websites used boxes where the visitor had to take an action to opt-out of being included for marketing. This is the current minimum requirement under PECR.
Whereas some had boxes that required an action to opt-in marketing, even specifying different possible channels, in line with ICO best practice recommendations.

Recommendation: Pharmacies should be aware of the upcoming changes to legislation that will mean that an organisation will have to be able to identify how consent to process information, or use information for marketing, was obtained. This will include greater detail such as the wording used at the time, the channel and date. There will be a requirement for customers to actively opt-in to grant consent by taking an action. Not changing a pre-ticked or unticked box will no longer be valid proof of gaining consent. By making changes now organisations will be able to assure themselves that their systems are ready for the changes.

→ GOVERNANCE

Findings:
Organisations with multiple branches were seen to have a program of regular monitoring in place such as a visit or audit. This may be part of a larger general check on the branch or specifically about data protection. They would include such things as:

- Checks on the filing of manual customer records.
- Checks on adherence to specified retention schedules.
- The security of information held on site.
- The availability of current procedures to staff.
- The availability customer information leaflets.
- That the training requirements for staff members are up to date, (if not monitored electronically from head office).

The better organisations conduct trend analysis of issues that are identified to determine if additional companywide steps are appropriate. These could be actions such as changing training materials or issuing reminders to branches.

Some organisations had a physical file on site holding a copy of the company IG policy and/or standard operating procedures. The better ones were seen to be short, concise and version controlled. Sign off sheets were present to ensure all staff members are familiar with the latest version of the policies.
Other organisations relied upon digital copies of material hosted on the company intranet being accessible by staff.

Commonly the policies covered subjects such as:

- Information Governance
- Customer Awareness
- Confidentiality
- Incident Management
- Records Management

Most large organisations had a written retention schedule for documents and records and in the best examples it was linked to an asset register. This retention schedule was normally managed by the individual pharmacies as the records were held on site. It was reported that smaller organisations, especially single site independents were the most likely not to have a written retention policy. However it was not clear if this is leading to excessive retention of unnecessary information.

Recommendation: Ensure that, in smaller organisations, retention periods for records containing personal data have been considered, are documented and staff are aware what records are to be retained, weeded and destroyed securely.

Several organisations operated online reporting tools for data protection incidents. These reports are sent to head office and as well as any specific action taken to address the issue, they are analysed for overall trends. This trend analysis is part of an ongoing risk management process.

→ SECURITY OF PERSONAL DATA

Findings:
Some sites operate a system where by visitors including contractors who may come into contact with personal data on site are required to sign a confidentiality agreement. This is in addition to confidentiality clauses in any third party contracts and is a good way of reminding the individual of their personal responsibility while on site.

Paper prescriptions are universally stored within the rear of the pharmacy prior to being collected, some within locked locations others not. Due to the monetary value to the business of prescriptions the monthly sending of bundles of prescriptions is well managed. The best seen involved a plastic mailing bag, or plastic bag inside a cardboard box to protect against moisture, coupled with pre-printed labels to ensure the correct address was used, and clear identification added to the exterior of the package so if the label became detached it could still be identified and returned to sender.

Confidential waste is generally handled well, either collected from the various branches by the company to be destroyed or on site using cross-

cut shredders. Where confidential waste is collected, the companies had taken steps to maintain the security of the material while in transit.

In some organisations fax machines still use the old style rolls that retain a negative of the information printed, or medicine label printers that use the same thermal transfer printing technology (as opposed to the direct thermal printing that uses thermochromatic paper). The negative imprints of the faxes and labels printed will therefore contain all the personal data inherent in those faxes or labels. Those organisations were aware of the inherent risks associated with such technology and all had requirements that used rolls be disposed of with other confidential waste.

Where fax machines are still in use within a business there was a variety of standards found. Some having clear policies in place covering their use which include using a fax cover sheet, calling ahead and after to confirm receipt and fax numbers for regular recipients are stored in the machine to prevent misdialling. However other businesses have no policies in place to ensure the secure use of faxes.

Recommendation: Faxes remain a high risk area for inappropriate disclosure of sensitive personal information. Ensure a mechanism such as “Safe Haven” procedures is in place to maximise the secure use of fax machines where there are no other alternatives and their use remains necessary.

Computer systems were an area of high variability. There was a large difference over access relating to the computer system, PMR and other software.

The majority of IT systems had a single company or branch logon to the computers in branch. From here the PMR system was accessed. Some organisations operated a single username and password for the PMR system allowing access to all staff. This means there are no audit logs created of viewing or amending records. At others each member of staff has a unique user logon and password. In the best examples these passwords expire after set time periods and must have a minimum level of complexity.

Recommendation: Systems that contain patient identifiable data should always have individual user logons to enable a full audit trail of view and change events to a customer record. Having an auditable log of changes and access to systems containing sensitive personal data is important to prevent illegal activity and maintain data quality standards.

In England some companies were able to act as issuing authorities for the NHS Smart Cards, while others were merely sponsoring bodies. It was seen that not all pharmacies have full compliments of eligible staff issued with

NHS Smart cards. This lead to situations where Smart Cards were not used appropriately and left logged in to systems to enable staff without cards to carry out EPS downloads.

Recommendation: There should be no situation where NHS Smart Card access is shared. All cards should only be used by the registered holder and systems activity audited solely to them alone.

Some businesses had a comprehensive standard operating procedure regarding staff leavers that included security matters such as returning keys, altering door or alarm codes and deactivating IT system permissions. However many did not.

Recommendation: Ensure a written procedure exists to identify actions to be taken when a staff member leaves. Ensure the prompt deactivation of IT systems access and that any codes they are party to are changed.

Some companies carried out a yearly review of their various systems' access accounts. This is a recommended procedure to be used in conjunction with a leaver's procedure to ensure the security of IT systems.

Backing up computer systems and the importance of maintaining the security of data seems well understood by organisations. Some had thin clients running off centrally operated servers, while others had independent PCs within branches. Those with onsite computers often use remote backups off site nightly to protect the information collected from loss. There were several reports that there is continued use of CD-RW or DVD-RW by independent pharmacies. Using such a system presents a complex and high risk. Access to the system that creates the copy must be strictly controlled to appropriate personnel. It must be encrypted in case of loss or theft. It should be kept in secure environmentally stable offsite storage. And the discs should be tested to ensure the data can be recovered should the need arise.

Recommendation: If using CD or DVD disks for backing up data ensure that the above points have all been considered and addressed.

Some community pharmacies are still using computers running Microsoft Windows XP. Extended support for Windows XP ended on April 8, 2014 after it stopped being sold in October 2010. That means systems running it have missed out on at least 30 important bundled security patches over the last two and a half years. Systems processing sensitive personal data should not be in this position. At some sites there is an ongoing process of upgrades to Windows 7.

Recommendation: Ensure that any computer processing sensitive personal data and connected to a network has been upgraded to a supported operating system.

There is a difference between approaches to internet security where some only allow computers to access to a limited white-list of acceptable internet sites. Others employ web filtering and anti-virus software. In larger organisations there are firewalls and antivirus programs set up to protect the servers. A small number of reports stated that their computer system that hosted the PMR has internet access but without web security leaving their data vulnerable. Viruses and malware are becoming more widely used to steal information, or hold computer systems hostage to blackmail their owners. Not having up to date antivirus software risks not only the customer's data but the business.

Recommendation: Ensure no networked computers are unprotected from cyber-attacks or malware.

Records on sites are generally stored in a range of files, box files and cardboard boxes depending on the branch.

There were several reports that there are not proper procedures and controls in place over removing personal data from the pharmacy. While details were not provided loss of data while in transit remains one of the most common breaches likely to lead to significant reputational damage or fines. It is important that this risk be removed wherever possible, and reduced elsewhere by having strict procedures in place. These procedures should be backed up with technological security such as encryption.

Recommendation: Ensure that a procedure is in place to control the removal of personal data from the pharmacy.

Community pharmacies visited had designed the layout of the branches with confidentiality in mind. Examples of good practice were:

- The placement of chairs so that customers waiting for prescriptions were situated away from the counter reducing the opportunity to overhear conversations.
- There is a separate collection area for prescriptions away from where a new customer may be discussing an issue with a Pharmacist.
- Counters designed so information was not viewable to customers.
- Windows that are viewable from public spaces were assessed to ensure that no customer information was viewable.
- Doors to consulting rooms were substantial enough to ensure the conversations within would not be overheard outside.
- Medication awaiting collection stored in a manner that prevented the names on the labels being read from the counter.

→ TRAINING

Findings:
All organisations visited provided their staff with training, both when they initially join and annually as part of a refresher program. Materials came from a variety of sources such as membership organisations, specialist in-house teams or external companies.

The most basic of training was for staff to read and familiarise themselves with the standard operating procedures used by the pharmacy. This was not always checked, and the staff's understanding of what they were reading was not tested. It was not clear if these procedures were regularly reviewed to ensure they contained the latest requirements.

A popular method was having physical version controlled policies and procedures on site with signature sheets to ensure all staff members had read them annually, and had seen any updated policies. These were checked on inspection visits and allowed the business to ensure all their staff had an understanding of the current requirements. This may be complemented with some eLearning modules for staff.

The most advanced online training platform seen involved individual accounts where each staff member could log in to see their personalised training requirements. From there they could undertake eLearning of the listed courses, the knowledge of which were assessed at the end. Statistics on completion results were actively monitored by head office to ensure that all staff members maintained in-date training and there was a process to chase up those failing in their obligations.

Some businesses also had articles that acted as reminders of data protection, confidentiality or IG as part of email campaigns or regular newsletters. Others used electronic noticeboards or background messages on computer screens.

A small number of single site independents reported that staff were provided with no training about confidentiality or information governance prior to being allowed to access patient identifiable data. Further there were several reports that staff did not need to complete yearly refresher training.

Recommendation: It is vital that staff have the training they need to carry out their work within the law. This means prior to handling any sensitive information they are trained in what they should and should not do. Training for staff on matters of security and confidentiality as it applies to their role should be refreshed yearly to prevent bad habits from developing. A program of regular spot checks or other mechanisms should

be employed to ensure staff are not putting the business at risk by breaching the DPA.

→ FAIR PROCESSING

Findings:
Many of the business provided their customers with varying degrees of fair processing information about how their information would be used.

The most popular was an in-branch leaflet, often also including information on Freedom of Information and the right of Subject Access.

Where specialist services were offered some had a range of leaflets that include information on fair processing or data protection. A very good example of this was where as part of the registration for the EPS a form states that the mobile telephone number and email address supplied will be used to contact them about the prescription service only. This is kept separate from the tick boxes provided to allow customers to show marketing preferences via mail, phone, email and SMS.

All the businesses visited that had websites, whether they operated an interactive website or not, provided fair processing information on them. This may be as part of a general privacy policy or as a separate document. However it was noted that in a sizeable number it was often only a general privacy policy covering the use of information in relation to the website, rather than about how the business as a whole used personal information.

Recommendation: Organisations should where possible seek to provide their full fair processing information to customers on their website in addition to any specifically relevant for interacting with the website.

Several reports were received that that fair processing information was not provided to customers in any form.

Recommendation: Providing information about how personal information will be used is a key part of to the Data Protection Act and being legally compliant. As such fair processing information should be drawn up and made available. Guidance is available on drawing up a privacy notice on the ICO website.

Further recommendations

Some other points observed that have not so far been covered are summarised below.

→ **ICO registration lapsed.**

! Failing to register when required is one of the few criminal offences in the Data Protection Act. Checking your status is easily done via the ICO website.

→ **Records stored in vulnerable locations.**

! Paperwork containing personal information must legally be protected from unauthorised loss, destruction or sharing. Organisations should think about where their archived paperwork is stored.

→ **Keys "hidden" rather than properly secured.**

! Combination locked key safes are a cheap and easy solution to hiding keys under plant pots or in unlocked draws.

→ **3rd party contracts do not ensure the security of customer data by including obligations of the company to comply with high levels of security when handling materials.**

! Ensure that all external contracts from cleaners to shredding companies have signed undertakings to protect personal data they process or come across.

→ **A small number of reports stated that their CCTV also recorded audio.**

! The ICO guidance on the use of audio recording is clear that it should be only used in exceptional circumstances. We would expect a full privacy impact assessment to be on file justifying why audio recording was deemed necessary in these cases, and proper signage advising that CCTV with sound recording was in operation.

→ **Several respondents across all areas reported they had not received adequate guidance on disclosing information in the manners that they were required to do.**

! Guidance and clear training is essential as this is the area where breaches can easily occur and customers will be very aware of it occurring. Staff should not be afraid to query the correct procedure, and employers should be able to direct them to the appropriate information.

→ **There were two incidents where a pharmacy was approached with a view to accessing and using customer data. Neither did so.**

! While good news that this is not happening frequently that it continues means there is still a need for companies to be aware of the very serious consequences than can occur if they fail to handle customer data correctly.

Further guidance

The ICO has produced a range of guidance for organisations to use to better manage and secure their personal information:

- Guide to Data Protection
- Taking a positive approach to information rights
- Privacy notices
- A practical guide to IT security
- Checklist for handling personal information
- 'Think Privacy'
- Overview of the General Data Protection Regulation (GDPR)

Further assistance

The ICO also has a helpline with staff on hand to answer queries about data protection compliance on **0303 123 1113**.

Appendix One: Background – Community Pharmacies

The pharmacy workforce in the UK is made up of approximately 150,000 people, with approximately 50,000 registered pharmacists. There were 13,985 registered community pharmacies as of the end of 2016, of which 64.5 per cent are owned by organisations with five or more pharmacies. (*General Pharmaceutical Council Data & Insight Team*). There are 1.6 million visits are made to community pharmacies every day, and the number of prescription items dispensed in the community is more than one billion per year. (*Dept. of Health "Community Pharmacy in 2016/17 and beyond"*).

The scope of a pharmacy practice has expanded from its traditional roles to now include a wide range of services related to health care. This includes clinical services, reviewing medications for safety and efficacy, prescribing some medications, and providing drug information.

Under NHS England the Electronic Prescription Service allows for a prescription to be created digitally by a prescriber and downloaded for filling by a designated pharmacy or medical device supplier. Pharmacists also can be granted access to a patient's Summary Care Record. This is a basic summary of information held by the patient's GP relating to drugs which the patient has been prescribed, known adverse reactions to drugs and any known allergies.

Under NHS Scotland the Pharmacy Care Record is in place which uses the ePharmacy Message Store. The message store controls the encrypted messages between GP systems, Community pharmacy systems and NHS National Services Scotland. This system enables Community pharmacies in Scotland to provide a Minor Ailment Service, Acute Medication Service and Chronic Medication Service.

Under NHS Wales there is currently an ongoing introduction of the Choose Pharmacy project. Based around Choose Pharmacy computer system it provides for three key services, the Common Ailments Service, Discharge Medicines Review, and Emergency Medicine Supply.

Pharmacies keep records of patient interactions in a Patient Medication Record (PMR) system. These include ProScript, Nexphase, RxWeb and AnalystPMR. Information can be added originating from a variety of sources including:

- GPs surgeries.
- A paper prescription presented to the pharmacy to be filled.
- Conversations held with customers.
- Information submitted via websites.
- Checks on linked systems.
- Information from care homes or hospices
- The police