Draft Guidance on Data Protection for Pharmacists

Introduction

This guidance has been prepared in consultation with the Office of the Data Protection Commissioner. Its purpose is to outline some general principles of data protection and to provide guidance to assist pharmacists in their professional practice in accordance with Data Protection legislation. It considers data protection in the context of pharmacy practice including matters such as safeguarding patient confidentiality and decisions regarding the custody and disclosure of patient's healthcare records.

Professional Obligations

Pharmacists are required by law to obtain, process and maintain patient records in the course of their practice. They are therefore subject to a number of duties in relation to these records including those imposed by pharmacy[1], medicines[2] and misuse of drugs legislation[3]. Their practice must also be carried out in compliance with any other pertinent legislation, including data protections legislation.

Pharmacists must act in accordance with their statutory Code of Conduct. In keeping with the third principle of the Code, pharmacists must never abuse the position of trust which they hold in relation to a patient and, in particular, they must respect a patient's rights, including their dignity, autonomy, and entitlements to confidentiality and information.

In addition, pharmacists should also be cognisant of their obligations to manage patient records appropriately in accordance with PSI Guidelines including the Guidelines on Managing the Closure and Cancellation of the Registration of a Retail Pharmacy Business.

Data Protection Obligations

The principal Irish law dealing with patient records is the Data Protection Act 1988 which was amended by the Data Protection (Amendment) Act 2003. The Acts set out the general principle that individuals should be in a position to control how data relating to them is used. The Acts also outline the legal responsibilities of being a **data controller** i.e. the individual or the legal person who controls and is responsible for the keeping and use of personal information. You are a data controller if you, as an individual or an organisation, collect, store or process any personal information about living people on any type of computer or in a structured filing system.

In addition to the personal data (e.g. addresses and PPS numbers) that pharmacists obtain, process and maintain, pharmacists also have access to "sensitive personal data." "**Sensitive personal data**" is

[1] The Pharmacy Act 2007 and regulations and rules made under that Act
[2] The Irish Medicines Board Act 1995 and regulations and rules made under that Act
[3] The Misuse of Drugs Act 1977 and regulations and rules made under that Act

defined under the Data Protection Acts to include data relating to patients' physical and/or mental health. All "sensitive personal data" is subject to additional obligations under data protection legislation.

Pharmacists and pharmacy owners must therefore ensure that the management of all data or information they collect, record or retain is in accordance with the Data Protection Acts 1988 and 2003. Superintendent pharmacists are responsible and accountable for the governance of data relating to patients' health in the pharmacies that they are responsible for. Pharmacy owners are responsible for ensuring that their superintendent pharmacists are facilitated and supported in ensuring that they can effectively discharge their professional responsibilities in these areas. Pharmacy owners together with pharmacists are responsible for ensuring the principles of data protection are met in the records they hold in pharmacies.

Full information on the provisions of the Data Protection Acts, including answers to frequently asked questions and a self-assessment checklist, is available from the Data Protection Commissioner website (www.dataprotection.ie).

Please note this guidance is not intended to cover every data protection scenario and does not give specific legal advice; pharmacists and pharmacy owners should seek the advice of the Data Protection Commissioner and/or their legal advisors if they have questions regarding specific issues.

1. Registration

Certain categories of data controller are required to register with the Data Protection Commissioner including health professionals processing personal data related to mental or physical health. In practice, all Retail Pharmacy Businesses must register with the Data Protection Commissioner. Guidance on registration requirements for data controllers can be found at www.dataprotection.ie

2. Information Governance

A system for the governance of personal and sensitive information should be established in each pharmacy. Superintendent pharmacists should make certain that pharmacy policies and procedures ensure compliance with data protection legislation.

3. The Eight Principles of Data Protection

All data controllers must comply with the following eight principles of data protection when they collect and use personal information. Therefore pharmacists should handle personal data in line with these principles regardless of the nature and purpose of the data obtained e.g. information held on a PMR, vaccination records or online interactions.

Table 1: The Eight Principles of Data Protection

Principle 1.	Obtain and process information fairly
Principle 2.	Keep it only for one or more specified, explicit and lawful purposes
Principle 3.	Use and disclose it only in ways compatible with these purposes
Principle 4.	Keep it safe and secure
Principle 5.	Keep it accurate, complete and up-to-date
Principle 6.	Ensure that it is adequate, relevant and not excessive
Principle 7.	Retain it for no longer than is necessary for the specified purpose or purposes
Principle 8.	Give a copy of his/her personal data to an individual, on request

More information on these principles can be found at: www.dataprotection.ie

Principle 1. Obtain and process information fairly

Pharmacists should ensure that each person about whom data is obtained and processed has full knowledge of and consents to the recording and keeping of data and understands what this entails. Considerations in determining if data has been obtained fairly **include** if the person is aware of:

- What information is being collected.
- The purpose in collecting the information.
- The persons or categories of persons to whom the information may be disclosed.
- The consequences of not providing the information.
- The existence of the right of access to their personal data.

When processing sensitive personal data, pharmacists must have the explicit consent of the patient. Consent can be understood to be explicit where a person volunteers personal data after the purposes in processing the data have been clearly explained. Pharmacists should consider displaying a notice which explains to patients the purposes of collecting and processing their data.

Principle 2. Keep it only for one or more specified, explicit and lawful purposes

Pharmacists should ensure that:

- The person knows the reason(s) why you are collecting and retaining their data.
- The purpose for which the data is being collected should be a lawful one.
- They are aware of the different sets of data which they keep and specific purpose of each.

Pharmacists should have a clear and legitimate purpose for collecting the personal information they gather.

Principle 3. Use and disclose it only in ways compatible with these purposes

When pharmacists and pharmacy owners obtain personal information for a particular purpose, they must not use the information for any other purpose e.g. patient contact data kept for the purposes of pharmacovigilance should not be used for marketing purposes.

Pharmacists must not divulge the personal data to a third party, except in ways that are "compatible" with the specified purpose. A key test of compatibility is whether you use and disclose the data in a way in which those who supplied the information would expect it to be used and disclosed.

Pharmacies should develop data disclosure procedures which establish the steps to be taken for both routine and non-routine disclosures. Such procedures should outline how decisions regarding disclosures are made and to whom questions regarding disclosure decisions should be addressed.

Principle 4. Keep it safe and secure

Pharmacists and pharmacy owners must take all reasonable care to protect personal information from unauthorised or accidental alteration, access, disclosure or destruction. Examples of suitable measures include:

Information Technology (IT) Measures

- Password protect access to computer systems. Keep passwords secure and regularly updated.
- Install and regularly update internet security software.
- Ensure robust back-up procedures are in operation.
- Position computer screens so that they are out of sight from visitors to the pharmacy and members of the public.
- Keep IT equipment containing patient data in the pharmacy. However if removal is required ensure data is encrypted and secure.
- Remove patient data from IT storage devices and computers prior to their disposal. Contact your system provider for the correct procedure to do this.

Communications Technology

- Encryption or a secure electronic pathway should be employed before email is used for the exchange of sensitive personal information.
- Pharmacists should take steps to ensure the security of information sent and received using fax machines. Suitable measures may include contacting the recipient by phone to check that they have received the faxed document or employing a fax cover sheet which clearly identifies the sender and intended recipient.

- Pharmacists should check caller authenticity before divulging personal information over the phone.
- Pharmacists should not use SMS or text messages for the transmission of sensitive information.

Physical Measures

- Lock filing cabinets when not in use.
- Any excess labels, receipts, used printer ribbon or paper containing patient's details should be rendered indecipherable or destroyed, in a manner appropriate for confidential material, prior to disposal.

Pharmacy Staff Measures

- Ensure staff are made aware of their responsibilities through appropriate induction training with refresher training as necessary.
- Ensure all non-pharmacist staff sign a confidentiality agreement that explicitly makes clear their duties in relation to patient confidentiality and personal information and the consequences of breaching that duty.
- Ensure access to personal/sensitive data is appropriately limited to staff as required for their level of participation in patient care.

Other Measures

- Take steps to ensure conversations about confidential information are not overheard e.g. through use of the patient consultation area.
- Do not leave confidential information where it may be seen or accessed by patients/the public.
- If you have concerns about the security of personal information at your place of work raise these concerns with the superintendent or supervising pharmacist.

Security Breaches

A data breach is an incident in which personal data is compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Examples include leaving a prescription on view in a public area or faxing a medical record to the wrong doctor. Should pharmacists or pharmacy owners become aware of a breach of personal data security they should ensure that appropriate actions are taken in line with the "Personal Data Security Breach Code of Practice" which can be found at www.dataprotection.ie. Pharmacy procedures should outline how this code of practice is implemented in the pharmacy

"Cloud" Storage and External Data Processors

Use of "cloud" data storage and/or external data processors requires additional considerations; these include ensuring that the data will be held securely. The Data Protection Acts place responsibility for data security squarely on the data controller who is accountable to the individual for the safeguarding of their personal information. Therefore a data controller must be satisfied that personal data will be secure if it is outsourced to a cloud provider or processed by an external data processor. Consequently the data controller will need to enter into written contract(s) with any cloud provider, data processor and/or sub-processors. Further information on "cloud" storage and contracts with data processors can be found at www.dataprotection.ie.

Principle 5. Keep it accurate, complete and up-to-date

The maintenance of accurate patient records is essential to the provision of quality and safe patient care. Pharmacists should ensure that records are maintained in such a manner so as to ensure their accuracy, completeness and currency.

Under Section 6 of the Data Protection Act, patients have the right to rectification and erasure of incorrect factual information. Where information is materially and significantly amended or deleted, pharmacists should notify any person to whom it was disclosed within the previous 12 months, unless such notification proves impossible or involves disproportionate effort.

Principle 6. Ensure that it is adequate, relevant and not excessive

Pharmacists should seek and retain only the minimum amount of personal data needed to achieve their purpose(s) i.e. data required under legislation or data kept in the interests of patient health, safety and/or for pharmacovigilance purposes.

Principle 7. Retain it for no longer than is necessary for the specified purpose or purposes

Personal data should not be held for longer than is necessary for the purpose(s) for which it was obtained. Minimum retention periods are legally required for some pharmacy records, for example in accordance with the Medicinal Products (Prescription and Control of Supply) (Amendment) Regulations 2011, Regulation 10 of the Medicinal Products (Prescription and Control of Supply) Regulations 2003 (S.I. No. 540 of 2003) and the Misuse of Drugs Regulations 1988 (S.I. No. 328 of 1988).

In the interests of patient safety and ongoing patient care, it may be appropriate, and perhaps expected, to retain records beyond these minimum specified periods. Access to such data may be required for legal, insurance or other purposes at some time in the future; nonetheless patient data must not be retained indefinitely. Pharmacists should develop policies on retention periods for all items of personal data which incorporate the statutory basis for retaining this data as well as information on how the data will be destroyed. It may be valuable to develop a destruction schedule which outlines and records when data is destroyed. If data is destroyed by an outside contractor, pharmacists should ensure that an appropriate contract is in place and should obtain a destruction certificate from the contractor.

Principle 8. Give a copy of his/her personal data to an individual, on request

Any individual, about whom you keep personal data, is entitled to request and obtain a copy of the data you are keeping about him or her.

To make an access request the individual must:

- Apply to you in writing (which can include email);
- Give any details which might be needed to help you identify him/her and locate all the information you may keep about him/her e.g. previous addresses, DPS/GMS numbers;
- Pay you an access fee if you wish to charge one. You need not do so, but it cannot exceed €6.35.

In response to an access request you must:

- Supply the information to the individual promptly and within 40 days of receiving the request;
- Provide the information in a form which will be clear to the average person, e.g. any medical abbreviations must be explained.

The right of access does not include a right to see personal data about another individual, without that other person's consent.

However, it is important to note that the Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989) provide that health data relating to a patient should not be made available to the patient, in response to an access request, if that would be likely to cause serious harm to the physical or mental health of the patient.

4. Disclosure of Confidential Information

In the course of their practice, pharmacists are regularly requested to share patient's healthcare records or information. Doctor's, carers and family members are often the source of such requests; they may ask for information to be provided verbally, in writing and/or electronically. Guidance for pharmacists on their decisions regarding such disclosures, with or in the absence of patient consent, is provided below.

4.1. Disclosure with Patient Consent

Pharmacists should obtain explicit patient consent prior to the disclosure of confidential information. Pharmacists should ensure that the patient understands what information will be disclosed, the purpose of the disclosure and to whom it will be disclosed.

If a patient refuses to give consent for information to be shared with other healthcare professionals involved in their care, it may impact on the quality of care provided to them. Pharmacists should inform patients of the potential implications of such a refusal.

4.2. Disclosure in the Absence of Patient Consent

In certain limited circumstances obtaining patient consent may be impractical, not possible, or undesirable. Section 2(1)(c) of the Data Protection Acts, provides that a data controller shall not further process personal data (which includes disclosure to a third party), except in ways that are compatible with the purpose for which the data was obtained. However, Section 8 of the Acts outlines the circumstances where exemptions to this rule apply.

Section 8 lifts the restriction on disclosure in certain situations, so that disclosures may be made in cases where the individual's right to privacy must be balanced against other needs of civil society, or where the disclosure is in the interests of the individual. In line with section 8, the circumstances where a decision to disclose in the absence of consent may be appropriate include:

- Where the disclosure is required by law, this includes disclosure to an authorised officer (inspector) of the PSI in the course of an inspection or investigation.
- Where the disclosure is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board.

(It is a matter for the data controller: (i) to satisfy itself that the provisions of this section of the Act are met, for example by establishing the bona fides of the authority and by obtaining assurances that the disclosure is actually necessary, and not merely of side interest, for the investigation of an offence; and (ii) to decide whether or not to comply with the request for disclosure. While section 8 lifts the restrictions on disclosure to a law enforcement or tax collecting authority, it does not impose any obligation on a data controller to comply with the request for disclosure.)

- Where the pharmacist believes the disclosure is required urgently to prevent injury, other damage to the health of a person, or otherwise to protect the vital interests of the patient (e.g. in response to a request from another healthcare professional for a patient history when a patient is seeking or undergoing medical treatment, or submission to the Irish medicines Board regarding an adverse drug reaction) or serious loss of or damage to property.
  (This does not authorise disclosures of personal information for general health research purposes, or for other medical purposes where there is no immediate or urgent risk to someone's life or health. In such cases, the normal data protection rules apply.)

Coming to such a decision can be challenging; in doing so a pharmacist should:

- Ensure that the person requesting the information has a legitimate reason for such a request.
- Consider the urgency of the request. It may be appropriate to take time to reflect before coming to a decision. In other situations a delay may not be appropriate.
- Consider requesting additional clarifications from those seeking information or consider asking for the request to be made in writing.
- Consider the possible harm to the patient or the public that may be caused by either disclosing or not disclosing the information.
- Seek advice from the Data Protection Commissioner and/or their legal advisors, when in doubt.

The primary principle of the Code of Conduct for pharmacists states that the practice by a pharmacist of his/her profession must be directed to maintaining and improving the health, wellbeing, care and safety of the patient. Decisions regarding disclosure should be made in light of this principle and on a case-by-case basis.

Where a decision to disclose is made, in the absence of consent, pharmacists should only disclose the information needed for the specified purpose. In such cases pharmacists should record who made the request, what information was disclosed and the reasons for their decision to disclose.

Information on disclosures permitted under section 8 can be found at www.dataprotection.ie.

4.3. Disclosure in Particular Circumstances – In accordance with Section 8 of the Data Protection Act

Disclosure to a Medical Practitioner, Pharmacist, Nurse or Dentist:

Disclosure includes verbal, written and electronic communications. In such cases the patient's consent should be obtained prior to disclosing health information, bearing in mind the provisions for disclosure without consent as outlined above (Section 4.2). Pharmacists should ensure that their decisions regarding disclosure are cognisant of their requirement to maintain and improve patient health and safety.

Disclosure to Parents/Guardians: A patient of 16 years or older has the right to refuse access to their medical records by a parent or guardian. Below that age, the pharmacist should exercise professional judgement, on a case by case basis, on whether, in the best interests of the child, the entitlement to access should be exercisable by the child alone, a parent/guardian alone, or jointly by the child and parent/guardian.

Disclosure to the Gardaí: Disclosure of the minimum required information would be appropriate where it is required for the purpose of preventing, detecting or investigating offences or apprehending or prosecuting offenders or in accordance with a court order.

Disclosure to Environmental Officer: It may be appropriate to obtain the officer's identification and written confirmation of the offence that they are investigating before disclosing the required information.

Shared Electronic Patient Records: Sharing electronic patient records, including with other healthcare professionals, constitutes disclosure. In such cases the patient's consent should be obtained prior to any disclosure. Therefore any shared electronic patient records should be fully in compliance with Data Protection legislation.

Deceased Patients: The rights to access under the Data Protection Acts only apply to the personal data of living individuals. Pharmacists should nonetheless maintain patient confidentiality after the patient has died. There are occasions when disclosures may be required by law or in the public interest. In such circumstances, given the inability to consult with the deceased patient, it may be appropriate to consult with the patient's next of kin and/or seek legal advice on the appropriateness of the disclosure.

Providing Medication Printouts to Patients' Family Members or Solicitors

With the patient's consent to disclosure of specified information to a specified person, pharmacists can provide such information to the agreed person. However, if the patient is not in a position to consent to the sharing of their information, it would be best to contact the Data Protection Commissioner or your legal advisors for advice on the requirements in such an instance.

5. Direct Marketing

If a pharmacy is involved in direct marketing activities, they must ensure that individuals are made fully aware, at data collection stage, of all the uses the organisation will make of their personal information. In such cases pharmacies should obtain the consent of the individual to use their personal data for direct marketing purposes.

Specific regulations govern electronic direct marketing communications (phone, fax, email or text) which require that an individual gives clear consent before any electronic communications, of a marketing nature, can be sent to them. In such cases pharmacies should ensure that they are in compliance with the legal requirements in this area and that they have obtained prior consent. Opt-in consent is required for the sending of an electronic marketing communication and there must be a valid opt-out contained within each marketing message sent. If the recipient does opt-out, their preference must be acted upon including removal from the marketing database. Further information can be found at www.dataprotection.ie.

6. Transfer of Patient Records on the Closure of a Pharmacy

Transferal of patient records constitutes a disclosure therefore pharmacists and pharmacy owners should ensure that such disclosures are carried out in line with Data Protection legislation.

The PSI has set out, in its Guidelines on Managing the Closure and Cancellation of the Registration of a Retail Pharmacy Business, appropriate measures to facilitate patients' access to their records.

Where the pharmacy is putting a system in place that would involve the transfer of patient records to another pharmacy, patient consent for these arrangements should, where practicable, be sought and given. Therefore, superintendent and supervising pharmacists should ensure all relevant patients are identified and contacted. The contact details of the pharmacy to which records will be transferred should be conveyed to the patients. Patients should be informed that they can choose an alternative pharmacy and the locations of alternative pharmacies should be conveyed to patients.

Self-Assessment Checklist

This checklist is designed to be used as a self-audit tool to aid compliance with the important elements of this guidance and to assist superintendent and supervising pharmacists in drawing up the relevant policies and SOPs. The checklist captures many important elements of the guidelines; it is not exhaustive and should only be used to assess pharmacy practice in combination with these guidelines and all other relevant guidelines, legislation and requirements.

A comprehensive self-assessment checklist is available from the Data Protection Commissioner's website and should also be used by pharmacists and pharmacy owners to assess their compliance. Please see: http://www.dataprotection.ie/docs/Self_Assessment_Data_Protection_Checklist/22.htm

Ask Yourself	Yes	No	N/A	Required Action
Is the pharmacy registered with the Data Protection Commissioner?				
Are all staff aware of who is the pharmacy's data controller?				
How does the pharmacy ensure that patients have consented to the recording and keeping of their data?				
Is the patient data the pharmacy holds secure?				
Do the pharmacy staff know their responsibilities and have they signed confidentiality agreements?				
Does the pharmacy have clear policies and procedures which ensure compliance with data protection legislation?				
Do I know what to do if someone asks for amendment of the information I hold about them?				
Do I know what to do if someone asks for a copy of the information I hold about them?				
Do I know what to do if someone asks for a copy of the information I hold about another person?				

Glossary of Terms Used

(From the Data Protection Commissioner's website www.dataprotection.ie)

Data

Information in a form which can be processed. It includes both automated data and manual data.

Sensitive personal data

Relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

Data Controller

Those who, either alone or with others, control the contents and use of personal data. Data Controllers can be either legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as G.P.s, pharmacists or sole traders.

Office of the Data Protection Commissioner

For further information, advice and guides on data protection issues, the Office of the Data Protection Commissioner can be contacted at:

Telephone: 057 868 4800
E-mail: info@dataprotection.ie
Address: Canal House, Station Road, Portarlington, Co. Laois
Website: www.dataprotection.ie