Allcare Pharmacy

Your Irish Community Pharmacy

Data Protection

&

Record Retention

Date of first issue	Jan 2013
Document Reference	CM001
Version	2.0
Revised Date	Revised Oct 2013

Allcare Pharmacy
Your Irish Community Pharmacy

Contents

Introduction

1.1 Context

At Allcare the privacy and data protection of our employees and customers is very important to us. The purpose of this policy is to provide guidance and best practice with regards to the handling of employee and customer data.

1.2 Purpose

This policy is devised to ensure that all personal data which is handled and/or retained within the pharmacy is done so in a manner which fully complies with the Data Protection Act 1988 and the Data Protection Amendment Act 2003.

1.3 Scope

This policy applies to all staff members including field staff members, third party and principle contractors. As such the policy must be briefed to all staff members and relevant third party and principle contractors. The policy will be reviewed annually or in the event of an adverse incident or change in legislation.

Procedure

2.1 Data Protection Definition

When a person gives their personal details to an individual or organisation, that person or organisation has a duty to keep these details private and safe. During the course of our business operations it is inevitable that we will collect personal and private data relating to our employees and customers. In order to safeguard this data there are eight rules of data protection which must be followed:

a) Obtain and process information fairly.
b) Keep it only for one or more specified, explicit and lawful purposes.
c) Use and disclose it only in ways compatible with these purposes.
d) Keep it safe and secure.
e) Keep it accurate, complete and up-to-date.
f) Ensure that it is adequate, relevant and not excessive.
g) Retain it for no longer than is necessary.
h) Disclosure of information.

2.1a Obtain and process information fairly

The data protection act requires that at the time of providing personal information individuals are made fully aware of:

- The identity of the persons collecting it. This is implied by the Pharmacy Building and information or personal data must only be collated by pharmacy staff members.
- To what use the information will be put. Patient and customer data may not be used for anything other than providing a health care service without the patient's or customer's written consent e.g. mailing lists, special offer e-mails etc.
- The persons or category of persons to whom the information will be disclosed. Patients and customers must be informed and consent to the disclosure of their personal data to a third party who is not directly responsible for the health care service of that patient or customer.

2.1b Keep it only for one or more specified, explicit and lawful purposes

Allcare will only keep data for a purpose(s) that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with that purpose(s).
Any person has a right to question the purpose for which we hold his/her data and we must be able to identify those purposes.

To comply with this the following must be adhered to:

- In general a person should know the reason/s why you are collecting and retaining their data. Customers must be informed if data is retained which is not necessary for the provision of health care services e.g. CCTV signage which states that the recording of footage is for the prevention of crime. The purpose for which the data is being collected should be a lawful one.
- You must be aware of the different sets of personal data which we retain and specific purpose of each.
    - Customer Data
        - Health Care Service Provision Data – Prescription and Services Data
          For the provision of adequate health care services and to maintain patient safety regarding the administration of medicines. This data is also retained to enable payment of relevant dispensing schemes through the PCRS.
        - Financial Data – Credit Card Slips
          For the accurate accountancy of transactions within the pharmacy. The identification of a person must not be achievable through the card information in the pharmacy e.g. only last 4 digits should be viewable on credit card slips.
        - Purchase Data – Customer Accounts
          To enable proof of identification and address in order for customer credit to be made available.
        - CCTV Footage
          To aid in the prevention of crime and to maintain the safety of customers.

- Staff Data
  - Personnel and HR Files
    To ensure the staff member is eligible to work
    To ensure the staff member's safety, health and wellbeing is maintained
    To provide the necessary training and performance management support required to complete their job role effectively.
    To enable payment of salary and applicable bonus payments.
    To provide a record of grievance, complaints or formal disciplinary incidents made by or against the staff member and subsequent investigations to allow for appeals process and adequate management and training of staff members.

  - CCTV and Covert Camera Footage
    To aid in the prevention of crime and to maintain the safety of staff members.

2.1c Use and disclose it only in ways compatible with these purposes

Any use or disclosure of information must be necessary for the purpose(s) or compatible with the purpose for which we collect and keep the data. You should ask yourself whether the person would be surprised to learn that a particular use of or disclosure of their data is taking place.

A key test of compatibility is:

- Do we use the data only in ways consistent with the purpose for which it is kept?
- As highlighted earlier in the policy customer and staff data must not be used for anything other than the purpose the data was originally intended for without the documented consent of the customer or staff member.

- Do we disclose the data only in ways consistent with that purpose?
  - Customers
    - Customers can request personal data relevant to themselves. This may be in the form of a dispensing report which details the medication supplied to them by the pharmacy over a given period of time.

- Customers may also request CCTV footage of themselves, all such requests must be made in writing and addressed to the Operations Department of Uniphar Retail Services. This is necessary as the release of footage must be processed in order to remove other identifiable persons from the footage.
- Files regarding an active investigation by the Gardaí or the company may not be released e.g. investigations relating to criminal activity.

- Staff
  - Staff members can also request personal data retained on file relating to their job or performance records. Requests must be made in writing through the Pharmacy Manager and authorised by the Business Manager.
  - Files regarding an active investigation may not be released e.g. investigations relating to criminal activity.

- Garda and External Authorities
  - On occasion the pharmacy may receive a request from the Gardaí or another external authority for documentation or CCTV footage. In these instances the purpose for the request must be obtained e.g. to aid a criminal investigation.
  - The footage must be signed for by the relevant member of authority prior to its release.
  - Your Business Manager must always be notified prior to the release of documentation or CCTV footage.

2.1d Keep it safe and secure

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The security of personal information is all-important.

The nature of security used may take into account what is available technologically, the cost of implementation and the sensitivity of the data in question.

A minimum standard of security would include the following:

- Access to any customer personal data, financial and sales data within the pharmacy to be restricted to trained and authorised staff, on a 'need-to-know' basis. Patient information must only be made available to qualified persons e.g. pharmacist, dispenser or technician.
- Access to computer systems should be password or bio-metrically protected to ensure unauthorised access is not achieved.
- Information on computer screens and manual files to be kept hidden from customers, contractors and unauthorised staff members.
- Back-up procedure in operation for computer held data, including off-site back-up.
- All reasonable measures to be taken to ensure that staff members are made aware of the organisation's security measures, and comply with them.
- The destruction of patient, customer, staff, financial, accounting and sales data must be disposed of in the correct manner. Shredding or the use of a confidential waste contractor must be utilised. Never dispose of documentation regarding sensitive information with general waste.
- The pharmacy manager is ultimately responsible for security and for periodic reviews of the measures and practices in place.

2.1e Keep it accurate, complete and up to date

Regular reviews of customer records and staff files must be conducted to ensure information held is relevant and up to date.

Best practice for reviews should include the following:

- Constant review of customer/patient files to ensure that information held is relevant e.g. DPS numbers, contact details and doctor details.
- Ensure that patient notes are updated regularly, for example if a patient is pregnant or breastfeeding.
- Staff files must be reviewed regularly and required updates made to personal details, for example next of kin, address and contact details.

2.1f Ensure that it is accurate, relevant and not excessive.

As discussed earlier in this policy data must not be used for anything other than the purpose the data was originally intended for. Patients and customers have a legal right to know what their data will be used for, why it is used and who will see it. They also should be made aware that data provided will not be used for marketing purposes, or to seek criminal proceedings or to sue for compensation.

Data collected must be the minimum amount of data required to be enable the pharmacy staff to complete the required task. Excessive data which is not relevant to the provision of health care must not be collected or held by the pharmacy in any form.

2.1g Retained for no longer than necessary

A record retention policy must be in place for your pharmacy and a formal procedure for the destruction of files must be adhered to. This is to ensure that patient, customer and trading information does not end up in the hands of unauthorised persons.

Records must be stored within the pharmacy under alarm coverage or sent for secure storage with an Allcare approved provider. Destruction of electronic files will be performed automatically by your software provider and manual files must be destroyed via shredding or a confidential waste provider.

Record Retention

- Epos, financial and cash processing audit parcels — 6 Years
  - Z-Totals
  - Customer Accounts
  - Cash Processing Sheets
  - Credit Card Slips
  - Petty Cash Receipts
  - Sales & Profit Reports
  - Epos Paperwork (refund slips, no sales etc)
  - FOC and Pharmacy Supplier Invoices
  - Services Invoices
  - MPS Daily Audit Reports
  - MPS Monthly Financial Reports
  - PCRS Books and Communications
- Regular Rx — 2 years
- CDs and CD register — 2 years
- Veterinary Rx and register — 5 Years
- High-Tech Rx — 3 years
- ULM Rx — 5 years

2.1h Disclosure of information.

Below is detailed a number of scenarios regarding the disclosure of information and the correct response to these requests.

- **Disclosure at the request of the individual to whom the personal data relates**
  A person seeking the disclosure of their personal data shall make their request in writing. Once submitted the data must be provided within forty days from receipt of the written request and that a fee currently set at €6.35 may be charged for the provision of such information.
  The request for personal data must come directly from the individual to whom the data and ID may be required to validate.

- **Disclosure at the request of a representative acting on behalf of the individual to whom the personal data relates**
  You may get a request for disclosure of personal data from a third party purporting to act as a representative of the person to whom the data relates. Such third parties include a spouse, a relative or a solicitor. Such requests should be accompanied by

written consent from the patient/customer concerned agreeing to the disclosure of their personal data.
There are some patients/customers who, because of illness or disability, may not be competent to give consent for the disclosure of their personal information. In such circumstances, the supervising pharmacist should discuss the request further with the person's next of kin and/or direct care givers.
Before disclosing data in such circumstances, the supervising pharmacist should also consult with the Superintendent Pharmacist. Where guardianship law is applicable, the rules for consent on behalf of patients with impaired competency should be followed.

- **Disclosure of a child's personal data at the request of a parent**
  Where a person is 16 years or older, he or she has the right of access their own personal information. Where the individual is below that age, the supervising pharmacist should exercise professional judgement, on a case by case basis, on whether the entitlement to access should be carried out by (i) the individual child alone; (ii) a parent or guardian alone or (iii) both child and parent/guardian jointly.
  Where the child is known to be in the care of the state or within a foster home the assigned social worker or foster parent becomes the legal guardian of the child.
  In making a decision, particular regard should be had to the maturity of the young person concerned to understand and make their own decisions about the handling of their personal health information, the involvement to date of the parent/guardian in their pharmaceutical care and the young person's best interests. Where there is cause for concern regarding a request for a child's personal data the supervising pharmacist may consult with the Superintendent Pharmacist for advice if desired.

Patients/customers withholding their consent for the disclosure of information
Patients and customers are entitled to withhold consent for disclosure to any third party of any information/form that identifies them, even if that party is a healthcare professional. As long as the patient is competent to make that decision and the consequences of this choice have been explained then no information should be disclosed.
Where there is a concern that the patient may suffer adversely if certain information is not disclosed, this should be explained to the person concerned and the matter formally recorded.

However, another lawful authority may in such circumstances allow or require disclosure of personal data. Possible scenarios relating to this issue are detailed below:

- **Disclosure of personal information in the absence of consent**
  - If requested by a member of the Garda Síochana not below the rank of chief superintendent or an officer of the Permanent Defence Force who holds an army rank not below that of colonel and is designated by the Minister for Defence under the Act, required for the purpose of safeguarding the security of the State
  - Required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting tax, duty or other moneys owed or payable to the State, a local authority or the Health Service Executive
  - Required in the interests of protecting the international relations of the State
  - Required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property
  - Required by or under any entitlement or by a rule of law or order of a court
  - Required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness
  - Made at the request or with the consent of the data subject or a person acting on his behalf

- **Declared disclosees**
  Your pharmacy is required to provide a list of persons or entities to which personal data may be disclosed to without consent of the person as part of the registration and renewal process. The list below is the recommended listing for your pharmacy.
  - Any medical/dental practitioner or nurse providing professional health care treatment
  - Person's next of kin
  - Person's direct caregiver
  - H.S.E
  - P.C.R.S
  - Department of Health and Children
  - Irish Medicines Board
  - The P.S.I.
  - An Gardá Síochána

2.2 PSI Code of conduct for Pharmacists

Pharmacists and those under the direction of the pharmacist engaged in the provision of pharmacy services must comply with the requirements as set out in the Pharmaceutical Society of Ireland's Code of Conduct for Pharmacists in particular:
"A pharmacist 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 and autonomy, and entitlements to confidentiality and information."

2.3 Training

Supervising pharmacists must ensure that all members of the pharmacy team are aware and demonstrate an understanding of their duty to maintain and respect a patient's, customer's and staff member's right of confidentiality. Staff members must read through this policy prior to being granted access to individuals personal data.

2.4 Registration with the Data Protection Commissioner

Registration of your pharmacy is initially completed centrally by Allcare Operations Department. This registration will require updating by the pharmacy on an annual basis. You will be notified by the operations department and provided with instructions for completion at the time of required renewal.

2.5 Support and Resources

Additional information regarding areas of data protection and record retention can be found through the following resources.

- The Pharmaceutical Society of Ireland; Code of Conduct 2009
  http://www.thepsi.ie/Libraries/Publications/Code_of_Conduct_for_pharmacists.sflb.ashx

- Data Protection Commissioner
  www.dataprotection.ie
  LoCall 1890 25 22 31

For support regarding specific queries or concerns please contact one of the below;

- Pharmacy Business Manager

- Allcare Operations Department 01-4287722

- Superintendent Pharmacist
  086 0216027