ePharmacy Toolkit for Community Pharmacists
Foreword

This toolkit has been developed by the community pharmacy IM&T facilitator group in order to support community pharmacists and their support staff in preparing for the Acute Medication Service (AMS) and the Chronic Medication Service (CMS) elements of the new community pharmacy contract.

It came about as a result of PCA(P)(2007)14 which outlined new contract preparation payment arrangements, requiring community pharmacists to undertake specific administrative tasks in preparation for the introduction of AMS and CMS.

The toolkit is divided into sections and these will be updated and added, to as and when, appropriate in relation to any specific new contract and ePharmacy Programme developments.

Each section consists of background information and references with supporting questions, standards and action recording. The expectation is that community pharmacists work their way through each section, complete the questions and then note any actions that they require to undertake. These actions can then be carried out over a period of time.

Completion of sections 1, 2 and 3 of the Toolkit fulfils the requirements set out in PCA(P)(2007)14 and the subsequent circular PCA(P)(2007)31 in terms of the following objectives:

- Patients records
- Data backup
- Data protection and patient confidentiality

The Community Pharmacy IM&T Facilitator Group
Useful Contacts

For your convenience we have included a contact sheet, please take a few moments to add useful contact details.

PMR Helpdesk Telephone No ________________________
PMR Helpdesk email ________________________
CP IM&T Facilitator Telephone No(s) ________________________
CP IM&T Facilitator email Address ________________________
ePharmacy Helpdesk Telephone No 0131 275 6600
ePharmacy Helpdesk email Address PSDHelp@psd.csa.scot.nhs.uk
Community Pharmacy Scotland 0131 467 7766
PSD Contact Office ________________________
Pharmacy Champion Telephone No ________________________
Pharmacy Champion email Address ________________________
Primary Care Lead Pharmacist Telephone No ________________________
Primary Care Lead Pharmacist Email Address ________________________
Director of Pharmacy Telephone No ________________________
Director of Pharmacy email Address ________________________
Introduction
The ePharmacy Programme
The ePharmacy Programme

The ePharmacy Programme is designed to support community pharmacists in delivering each of the core components of the community pharmacy contract which require an IT infrastructure (see Figure 1); the Minor Ailment Service (MAS), the Acute Medication Service (AMS) and the Chronic Medication Service (CMS).

<table>
<thead>
<tr>
<th>PHARMACEUTICAL SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minor Ailment Service (MAS)</strong></td>
</tr>
<tr>
<td>MAS enables people who are exempt from prescription charges, to register with a community pharmacy of their choice and have their common conditions treated by their community pharmacist on the NHS without the need to visit a GP</td>
</tr>
<tr>
<td><strong>Acute Medication Service (AMS)</strong></td>
</tr>
<tr>
<td>AMS continues to provide patients with access to the pharmacy of their choice for the dispensing of prescriptions</td>
</tr>
<tr>
<td><strong>Chronic Medication Service (CMS)</strong></td>
</tr>
<tr>
<td>CMS allows patients with long-term conditions to register with a community pharmacy and receive a system of personalised care which ensures they obtain optimal therapeutic benefit from their medicines and minimises any predictable undesirable effects.</td>
</tr>
</tbody>
</table>

Figure 1

Background

In 2001-2002 a pilot project was established within NHS Ayrshire & Arran PCT to develop a system to provide the necessary functionality for the **Electronic Transfer of Prescriptions (ETP)**. Stage I of the pilot was completed in the latter part of 2002-2003 and provided valuable lessons to inform a wider Stage II roll out of the pilot. As a result of the February 2002 publication of the pharmacy strategy (**The Right Medicine**), it was decided that the project’s objectives should be broadened to include the development of e-applications that would support the future delivery of the new community pharmacy contract and improve communications across the healthcare team.

To reflect the extended remit, the initiative as a whole was re-branded as the **ePharmacy Programme**. Since then there have been further policy and service developments that impact on the ePharmacy initiative, which is an integral part of the eHealth programme.

The Generic Architecture & Infrastructure

At the heart of the infrastructure is the **ePharmacy Message Store (ePMS)**, which is used as a control for encrypted messages between GP systems, community pharmacy systems and National Services Scotland (NSS) who own and support the information gateway. The ePMS supports all current e-service developments. It has
been designed on the basis that further system developments or changes can be accommodated where required, e.g. for the introduction of digital signatures etc. The standards and architecture used for this and all other system developments and interfaces are being developed in conjunction with national and European guidelines and within the overall direction of the national IM&T strategy so, for example, the data collected in ePharmacy transactions can be a contributor to the Electronic Health Record (EHR) in the future.

All community pharmacies have been connected to the N3 network as part of the infrastructure programme and this has allowed access to NHSmail and Anti-Virus software (see appendix 1 for further information).

Another infrastructure requirement has been the need for drug dictionary mapping functions to enable a common language between GP and pharmacy systems and NSS until such time as all systems use the UK agreed drug dictionary, the Dictionary of Medicines & Devices (dm+d). Around 80% of the most commonly prescribed drugs can now be mapped across the various systems currently in use. This allows for a more efficient system for processing ETP transactions and the automation of the payment process for reimbursement.

The current payment process for both remuneration (fees and allowances) and reimbursement (drug costs) is already automated to a degree whereby dispensed prescriptions are scanned by an optical reader and processed accordingly. The advent of ETP and drug dictionary mapping will see the introduction of ePay which will improve the efficiency of the current payment system by removing the reliance on paper processing. Good progress is being made on developing the ePay component which will also provide quicker and richer sources of data for NHS Scotland via data feeds to the Information and Statistics Division (ISD) of NSS.

A central Patient Registration System (PRS) has been developed in order to allow community pharmacists to register patients for two of the new contract services; the Minor Ailment Service (MAS) and the Chronic Medication Service (CMS). It uses the Community Health Index number (CHI) as the unique patient identifier.

Developments are also required on both the community pharmacy and GP IT systems in terms of ePharmacy functionality. This includes the distribution of digital certificates to authenticate valid message sources (i.e. the practices and pharmacies) and system application developments in terms of specific software enhancements.

There are six pharmacy Patient Medication Record (PMR) system suppliers servicing community pharmacies in Scotland and five GP clinical system suppliers. A key action in the ePharmacy programme has been the early engagement of all system suppliers to inform them fully of the strategic and operational direction of the programme. This initiative is going well with all suppliers demonstrating full commitment to the ePharmacy development process.
Support and Advice

Community Pharmacy IM&T Facilitators

The Community Pharmacy IM&T facilitators work to support community pharmacists and their staff in using the systems and applications to deliver ePharmacy. For example, they will be providing basic training and ongoing assistance on:

- Access to and use of N3 and NHSmail
- Applications to support ePharmacy
- Reporting and resolving problems

In addition there are GP IM&T facilitators working with GP practice/s to make sure that they are able to use ePharmacy applications installed on their systems.

ePharmacy Service Helpdesk

Practitioner Services Division (PSD) run the ePharmacy Service Helpdesk. It is designed to deal with calls relating to the operation of ePharmacy applications. **All technical or hardware issues should be initially directed to your PMR System Supplier and not to the PSD Helpdesk.** Queries regarding the Scottish Drug Tariff and product exemptions should be directed either to Community Pharmacy Scotland (CPS) or the appropriate PSD site (Bridge View, Savoy Tower and Elliott House), as at present, and not to the Helpdesk.

The ePharmacy Helpdesk aims to:

- Provide a single point of contact to record ePharmacy related calls.
- Provide a call management service that logs calls and assigns issues to an appropriate Resolver Group where required.
- Manage all calls through the Helpdesk system ensuring that the relevant information is retained/updated on all call progress. Customer Service Advisors will monitor calls and keep all relevant parties updated on call progress through to resolution.
- Work co-operatively with all Technical and PMR Helpdesks
- Advise on a PMR supplier issue by advising if the call enquiry needs to be transferred to the PMR suppliers Helpdesk.

Troubleshooting

If you are having any difficulties with your PMR system then first check the following:

- The PC, monitor and printer are plugged in and switched on
- All leads are connected properly and not loose e.g. monitor and printer cables, mouse and keyboard leads
- Ensure that the time settings on your PC are correct; failure to do so will affect your ability to communicate with ePMS
The New Community Pharmacy Contract

Minor Ailment Service (MAS)

MAS is a service that allows patients exempt from paying prescription charges to use their community pharmacy as the first port of call for NHS services for advice and treatment of common illnesses. Patients are registered for MAS on PRS electronically, using their CHI number, via N3 and ePMS. In addition any intervention from a MAS consultation (treat, advise, refer) is recorded electronically and sent to NSS providing the link to ePay for both remuneration and reimbursement purposes.

Acute Medication Service (AMS)

AMS is the provision of pharmaceutical care by community pharmacists for acute episodes of care. It also introduces the electronic transfer of GP10 prescriptions (ETP). A GP prints a GP10 prescription form which has a bar code and unique prescription number (UPN) and at the same time their system also automatically sends an electronic prescribing message to ePMS. The electronic message contains exactly the same information as printed on the GP10. On receiving a prescription in the pharmacy the pharmacist scans the bar code thereby pulling down the electronic message from ePMS. The pharmacist then uses the information in the electronic message for dispensing purposes, reducing the need for data entry and transcription. Dispensing a prescription triggers the creation of an electronic claim message which the pharmacist sends to ePMS from where it is accessed by Practitioner Services for payment processing through ePay.

Chronic Medication Service (CMS) (currently still being developed)

CMS is the engagement of pharmacists in the management of individual patients with long term conditions through improving their understanding of their medicines and working with them to maximise the clinical outcomes from their therapy. A patient registers with a community pharmacy for CMS on PRS again using the CHI number and the ePharmacy infrastructure. The pharmacist and patient then work together to address issues such as concordance. In addition, eCMS builds on ETP and allows a GP to produce a “master” serial prescription for a 6 month or 12 month period to be dispensed at regular intervals by the pharmacist. This serial prescription is again transmitted by ETP to ePMS from where it is retrieved by the pharmacist when the patient presents in the pharmacy. The pharmacist retains the serial prescription and scans it at the appropriate dispensing intervals to pull down the data. As with eAMS each dispensing episode triggers the creation of an electronic claim message which the pharmacist sends to ePMS from where it is accessed by Practitioner Services for payment processing through ePay. Once all the instalments from the CMS Master prescription are dispensed the pharmacist sends the Master prescription to Practitioner Services. There are clinical protocols that accompany the serial prescriptions which outline any monitoring requirements and feedback. The GP practice receives feedback on the dispensing of serial prescriptions and on any protocol monitoring requirements. This is in the format of compliance information straight into the GP system and a more detailed electronic feedback report. This happens, again, via the ePMS.
Section 01
Updating PMR Records
**Updating Patient Medication Records**

Accurate and up to date patient records are key to the pharmacist’s new roles within eAMS and especially eCMS to deliver ongoing patient care.

All contractors are therefore required, over the course of 2007/2008 to ensure that all fields in the PMR records which they hold are accurate and up to date, and that the total number of current patients can be readily identified.

This activity will reduce the possibility of duplicate records existing or being created.

Please use this section as a means of identifying patient records that require to be updated thereby ensuring patient records on your PMR system have accurate and meaningful data. This also means deleting any patient notes that you may include in your patient details such as reminders for patient delivery arrangements in the address field. If these are not removed then your system will not be able to match an address in the electronic message with a patients already held in your PMR system.

Some of the following functions may be performed / supported by your Head Office, such as data archiving and storing a patient medication record.

**Part 1 – Patient details required**

Each patient record should contain the following information. Place a tick against those that you record routinely:

<table>
<thead>
<tr>
<th>Details</th>
<th>Tick</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient’s name (this should be the name which would be used in formal communications e.g. when registering with their GP, birth certificate, passport or driving licences)</td>
<td></td>
</tr>
<tr>
<td>Patient’s address and full post code (with no additional free text entries e.g. prescription delivery messages)</td>
<td></td>
</tr>
<tr>
<td>Patient’s date of birth</td>
<td></td>
</tr>
<tr>
<td>GP practice details</td>
<td></td>
</tr>
<tr>
<td>Patient’s CHI number (the CHI number is a 10 digit number containing the D.O.B and a unique identifier)</td>
<td></td>
</tr>
<tr>
<td>Patient’s last advised exemption status. Some exemption categories may require to be checked each time you dispense a prescription.</td>
<td></td>
</tr>
<tr>
<td>Carer’s contact details where known (this may the only contact there is for the patient)</td>
<td></td>
</tr>
</tbody>
</table>

Capturing the above information will ensure that all patient records on your system have the appropriate details required for eMAS, eAMS and eCMS where applicable.
**Part 2 – Managing patient records**

To reduce the possibility of duplicate records ensure all staff are aware of how to:

- Search for a record
- Edit a record
- Merge a record if there is more than one entry
- Create a new record: what information is required and why (please refer to section one for explanation)

---

**Part 3 – System Reports**

Ideally it would be advantageous to be able to see the number of active patients using your pharmacy and what services you provide for them. However, at present, this information is not necessarily available as a report facility in all PMR systems.

- Is there a system report to identify all active patients’ records?

Details on this capability can be sought from your PMR Supplier.

---

**Part 4 – Archiving**

It is advantageous to archive old data from your system freeing up disk space and speeding up the backups and general system speed.

- Does your PMR have an archiving facility?
- Do you know how to access data from the archive?
Section 02
Data Backups
Data Backup

This section provides guidance on minimising the risk of a disaster involving a pharmacy computer(s) and what action to take to recover the system.

What is a data backup?

Backing up is a method of copying the data stored on the computer’s hard disk on to an external storage device so that if anything happens to the computer all the data from the old system can be restored in its entirety to a replacement system.

It is essential that the role and responsibilities for running your computer system backup are clearly defined and are allocated to a small number of individuals (more than one) who are well trained for this role. Good training to the necessary levels is an effective way of preventing (or minimising) disaster.

What is meant by a disaster?

A situation where all the data held on a pharmacy system was lost or corrupted would be described as a disaster. Such events could include:

- Faulty hard drive
- Fire
- Vandalism

The importance of backing up your data

Backing up data is often a task that is done only when you remember or have the time. However, have you considered how much time and money you invest in entering data on to your clinical system?

Now consider what you would do if it were all lost, stolen or the hard disk fails. If you never backup your system or data, when a disaster does occur you could find you lose several months or even years worth of information.

As you can see the importance of backing up cannot be stressed enough. The amount of disruption caused to all concerned in a disaster situation is so great that a good backup strategy should be high on the list of priorities.

Your pharmacy PMR system may force you to carry out a backup after a set numbers of days if you have not already done so. Or, as is the case with some of the pharmacy multiples, data backup may be supported automatic to a central backup system off-site.

Your backup procedure

This next section details questions that you should address within the pharmacy to help develop a backup procedure or evaluate an existing one.
Part 1 – Responsibility

To ensure the integrity of the backup system it is recommended that you have clearly defined roles for the process and each member of staff involved is aware of their individual tasks.

Question 1 – Who is responsible for data backup within the pharmacy?

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No one is currently designated in this role</td>
<td>One person currently has responsibility</td>
<td>The individuals (more than one) are indicated in a documented procedure</td>
</tr>
</tbody>
</table>

From this exercise consider any requirements that you can identify in your pharmacy to ensure that there are clearly defined roles and to make staff aware of the importance of the backup procedure.

Question 2 – Does your PMR supplier provide any information regarding data backups?

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not aware of any information</td>
<td>Yes</td>
<td>Yes and this has been reviewed and built in to the internal documented procedure</td>
</tr>
</tbody>
</table>

From this exercise review any supplier information and work towards inclusion in a written procedure.

Question 3 – Are there any other types of data stored on your computer excluding your PMR data e.g. compliance aid information, staff rotas, NHS Circulars etc. which require backup?

Make a list of any other data that you will need to ensure is backed up on a regular basis and include this in your backup procedures.
Part 2 – Storage

There are various data backup options available (outlined below). The key factors in selecting the correct one are:

- Reliability
- Capacity (storage space)
- Compatibility
- Budget

This might be dictated to you by your system supplier or I.T. Department.

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>What It Is</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| External drives       | A high capacity drive which may be removable and stores large quantities of data | • Includes backup software  
• Range of storage options  
• Portable | • Involves investment in terms of hardware and in some cases disks as well |
| CD-RW                 | A compact disk onto which data is burnt using a CD-RW drive. (RW stands for “re-writable”) | • Can hold up to 700MB  
• Portable  
• Re-useable  
• Disks are relatively cheap | • Requires a CD-RW drive  
• Older CD players can’t read CD-RW disks  
• Data can be accidentally overwritten |
| DVD-RW                | A DVD onto which data is burnt using a DVD-RW drive.                      | • Newer computers are supplied with DVD-RW drives  
• Flexible as can also be used to burn CDs  
• Holds up to 4.7 gigabyte  
• Portable  
• Re-useable | • Requires a DVD-RW drive  
• Might have to buy software  
• Data can be accidentally overwritten |
| USB flash drive       | Similar to a small hard drive that plugs in via the USB port on your computer. | • Portable  
• Holds up to 64 gigabytes or more  
• Files can be saved, modified and deleted  
• Prices are relatively low | • Very small and can be easily lost  
• Can fail or become corrupted  
• Data can be accidentally overwritten |

**NOTE:** under NO circumstances should data be backed up to the c-drive.

Question 4 – What storage device do you use for backup purposes?

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know or None</td>
<td>A small capacity option requiring multiple disks</td>
<td>An option that provides enough capacity to store all data in the one place</td>
</tr>
</tbody>
</table>
Part 3 – Backup Routine

It is recommended that a cyclic backup routine should be employed, in other words more than one backup device. This means that if the last copy of your data is lost or corrupted you will still be able to restore from further back in the history.

An example of a very simple cycle based on 3 discs might be:

<table>
<thead>
<tr>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
<th>Sunday</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk 1</td>
<td>Disk 2</td>
<td>Disk 3</td>
<td>Disk 1</td>
<td>Disk 2</td>
<td>Disk 3</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Disk 1 should be clearly marked as Mon/Thur

Disk 2 should be clearly marked as Tue/Fri

Disk 3 should be clearly marked as Wed/Sat

To avoid confusion label disk and not the case (remove the case insert and you can see through the case lid.) You may also wish to consider having a spare disk for ad-hoc backups or for replacement purposes.

**Question 5 - Do you cycle your back up media?**

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>2-3 disks are used</td>
<td>1 disk for each working day</td>
</tr>
</tbody>
</table>

Based on this exercise consider your current backup routine. If it is not based on the cycling of storage media review it and detail plans to address this requirement.

**Question 6 - Do you clearly mark your backup disks etc.?**

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes each is clearly labelled</td>
<td>Each is clearly labelled and relates to a backup log</td>
</tr>
</tbody>
</table>

If backup disks are not clearly marked take steps to remedy this.

**Question 7 – Do you have a schedule for replacing your backup disks?**

Backup disks should be replaced periodically to reduce the risk of backup failure. Old disks should be securely wiped using software that prevents any recovery of data.
Part 4 - Frequency of backups

Ideally a backup should be made at least once every working day, preferably at the beginning or end to ensure that the maximum amount of data is stored. The longer the interval between backups, the more data will be lost in the case of system failures (e.g. a hard drive failure).

If a backup is not performed at the scheduled time it should be carried out at the earliest opportunity, but never missed out altogether.

Question 8 – How often do you backup your data?

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data is never backed up</td>
<td>On a regular basis e.g. weekly</td>
<td>Daily</td>
</tr>
</tbody>
</table>

From this exercise review your current backup frequency and if necessary detail plans to put in place appropriate scheduling.

Question 9 – Does your system offer automated backups?

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know or No</td>
<td>Yes, but staff are not aware of how it is configured</td>
<td>Yes, and it is used to schedule daily backups at an appropriate time</td>
</tr>
</tbody>
</table>

From this exercise identify tools within your pharmacy system to facilitate the running of regular backups.

Part 5 – Storage

The most secure way of storing backups is to remove them from the pharmacy site altogether. However, if this is not practical, backups should be stored in a fireproof safe or cabinet along with the log book. If they are not stored properly then there is little point in having a backup routine in place.

Disks etc. should always be stored in a protective case and never left loose.

Question 10 – Where do you store your backups?

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No designated area</td>
<td>In a designated area within the pharmacy</td>
<td>A fire proof safe with the log book or off-site storage</td>
</tr>
</tbody>
</table>
Review current storage of backup discs and ensure that staff involved are fully aware where they should be kept.

Part 6 – Log book

A log book encourages a systematic approach to be taken to backups which is vital if a successful restore is required at any point. The log book will be one of the first sources of information that is checked after a disaster is reported. As a minimum a record should detail the following:

- The date and time of the backup
- How the backup was run
- Any unusual events during the backup process
- The sequence of disks used
- Changes to computer software etc.

This information may isolate the source of a problem and if dormant for some time it will tell you what the last reliable backup was.

If discs etc. are not used in the order they were intended, the log book will be the only method to match which day’s data was stored on which tape.

A suggested template for simple log is shown below and a blank copy included in the appendix 2 for your use.

<table>
<thead>
<tr>
<th>Date</th>
<th>Tape</th>
<th>Auto/Manual</th>
<th>Time</th>
<th>Status</th>
<th>Comments</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/11/07</td>
<td>Mon/Thur</td>
<td>Auto</td>
<td>17.00</td>
<td>Successful</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/11/07</td>
<td>Tue/Fri</td>
<td>Auto</td>
<td>17.00</td>
<td>Successful</td>
<td></td>
<td></td>
</tr>
<tr>
<td>07/11/07</td>
<td>Wed/Sat</td>
<td>Manual</td>
<td>14.00</td>
<td>Successful</td>
<td>Software upgrade</td>
<td></td>
</tr>
<tr>
<td>08/11/07</td>
<td>Mon/Thur</td>
<td>Auto</td>
<td>17.00</td>
<td>Successful</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Question 11 – Do you currently utilise a log for data backups?**

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Sometimes if we remember</td>
<td>A log is always completed after each backup</td>
</tr>
</tbody>
</table>

From this exercise and sample log consider any requirements that you can identify for the logging of backups and put in place plans to implement an appropriate solution.
Part 7 – Failed backups

The primary causes of a backup failing are as follows:

- Operator error i.e. omission or incorrectly scheduled time.
- Disk error
- Hardware error
- Software error
- Unforeseen circumstances e.g. power failure

If an error is detected the system supplier should be contacted and advice sought on the next course of action before a critical failure becomes apparent.

If the cause of the backup failure can be determined two options are available:

1. Wait until the next scheduled backup time and ensure that the backup is done correctly.
2. Repeat the backup immediately.

The correct option will depend on the workload currently being undertaken in the pharmacy and the time that the failure is discovered.

**Question 12 – Are the staff involved aware of how to check that your PMR and other data backups have been successful?**

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>The steps to be taken are detailed in a written procedure</td>
</tr>
</tbody>
</table>

Based on the exercise above work towards training all staff involved on how to check that a backup has completed successfully.

**Question 13 – Are staff aware of the steps that should be taken if a failed backup is identified?**

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard – Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>The steps to be taken are detailed in a written procedure</td>
</tr>
</tbody>
</table>

Based on the exercise above work towards detailing the correct steps to be taken in a written procedure.

**Question 14 – Are backups tested on a routine basis to ensure that data can be restored from the backup?**
Securing the computer system

If the pharmacy computer is stolen the loss of the data on it is more significant than losing the hardware itself. Regular backups of the data will enable a new system to have the pharmacy data restored on to it. However, even if the data has been secured the theft of the computer system causes such disruption that every effort should be made to avoid this.

Hints & Tips

- Never leave portable/notebook computers unattended.
- Before selling or scrapping obsolete computers ensure that all pharmacy data is securely removed from the system using appropriate software to prevent any subsequent retrieval of the data.
- PC alarms are available and work in such a way that if a computer is disconnected and moved the internal alarm goes off and won’t switch off until the power supply has been reconnected. Some PC alarms may be connected to the building alarm system.
- Always check the credentials of people working on or removing your equipment.
- If a hard disk is being replaced by engineers always ensure that the system supplier disposes of the failed hard disk properly to ensure that any practice data remaining on it is destroyed.
- Always keep software disks locked away securely.
- To make the theft of memory chips as difficult as possible, keep the computer case locked at all times. If the computer case is locked ensure that the keys are not stored near by.
- Securing brackets can be used to effectively bolt the computer case to the desk/worktop.
Caring for equipment

One cause of a computer system failing can often be as a result of careless treatment of equipment cabling. Cables are a weak link in any electrical equipment and they are often overlooked as a possible cause of failure:

Hints & Tips

- Always connect cables to computers and peripherals before switching on at the main power supply.
- Ensure that cables connecting into the computer and peripherals are attached securely.
- Place cables away from areas where they could be accidentally kicked/pulled out of their sockets.
- Ensure that covers or labelling exists on plugs and sockets to ensure that computer equipment is not switched off accidentally, causing an uncontrolled shutdown.
- The use of domestic multi-socket mains adapters for critical items of computer equipment is common but not recommended.
- Ensure that computer equipment is securely plugged into wall sockets.
- Never rest furniture or other heavy items on cables.
- Cables should not run across floors where people walk.
- Care should be taken to insert shaped connectors into ports in the correct way to avoid damaging the connecting pins.
- If using multi-plugs ensure that they are surge protected
Section 03
Data Protection & Patient Confidentiality
Data Protection and Patient Confidentiality

The following section covers Data Protection and Patient Confidentiality. It starts with an introduction to the various legal requirements and information sources which you may wish to review in more detail.

Patient Confidentiality

Patients expect that the information they supply about themselves, that is discovered during the course of their care or that is held about them, is kept confidential. The introduction of more electronic data recording and sharing, such as a future national Electronic Health Record (EHR), requires the necessary safeguards to be built in to allow access to the appropriate data by the appropriate professionals whilst preventing unauthorised access by others.

The Caldicott Committee Report outlined principles of good practice to safeguard confidentiality including:

- Justify the purpose for the use of the data
- Do not use patient identifiable information unless absolutely necessary
- Use the minimum necessary patient identifiable information
- Ensure that everyone with access to patient identifiable information is aware of their responsibilities.

Each NHS Board has a Caldicott (or Information) Guardian. They are a senior clinician, normally the Medical Director or Director of Public Health. Their responsibilities include:

- Auditing current practice and procedures
- Developing protocols for inter-agency information sharing at a local level
- Making decisions about how their organisation uses patient identifying information.

Data Protection Act 1998

The Data Protection Act is a UK Act which regulates the processing of personal data. It sets out a number of data protection principles to which all organisations processing personal data (data controllers) must comply. It covers both computerised and manual records for living patients. Amongst other things, these principles regulate the fairness and lawfulness of the processing, the accuracy of the data and the purposes for which the data may be processed, the time for which the data may be retained and the need for security. Each NHS Board has a Data Protection Officer from whom health professionals and other staff can seek advice on all aspects of data protection and confidentiality.

The Freedom of Information (Scotland) Act 2002

The Freedom of Information Act (FoIA) gives a general right of access to all types of recorded information held by public authorities, including community pharmacies. The Act imposes two main responsibilities; a public authority must produce a publication scheme (effectively a guide to the information that they hold that is
publicly available) and they must deal with individual requests for information. The duty to adopt a publication scheme came into force on 31 October 2003 and the requirement to deal with requests for information on 1 January 2005. Community pharmacies should make their publication schemes available, for example, in hard copy or on a web site.

This Act extends a person’s rights under the Data Protection Act to allow access to all types of information that may be held, both personal and non-personal, although there are some exceptions which are exempted. Anyone can make a written request (including an email request) for information which must give the applicant’s details and the information sought. In general a public authority then has up to 20 working days in which to respond to the request for information.

Further background

A number of useful documents and web sites are listed below to provide further background information on data protection and patient confidentiality and how they relate to community pharmacy.

Document 1 – NHS Code of Practice on Protecting Patient Confidentiality. All staff and contractors to the NHS have a duty to maintain the confidentiality of personal health information. This document sets out the code of practice for patient confidentiality within the NHS and provides guidance on handling personal health information across a range of healthcare settings.

You should familiarise yourself and your staff with it’s contents. You may wish to print off a copy and include it in this Toolkit.


Web Site – NHSScotland Confidentiality and Data Protection. This web site provides additional reading on the subject. You can also download the NHS Code of Practice, mentioned above, from here.

This site contains information on the ways in which the NHS protects the personal data that is needed to provide health care services.

It provides information on the basic principles of data protection, links to additional resources and guidance and training

http://www.confidentiality.scot.nhs.uk/
This document outlines your professional responsibilities and legal duties with regards patient confidentiality. It provides mandatory standards and best practice.

http://www.rpsgb.org.uk/pdfs/coepsgpatconf.pdf

This document outlines your professional and legal duties to obtain a person’s consent for the professional services, treatment or care you provide as well as for the use of any patient information or data. As with the previous document it provides mandatory standards and best practice guidance.

http://www.rpsgb.org.uk/pdfs/coepsgpatconsent.pdf

Document 4 - Royal Pharmaceutical Society of Great Britain *Confidentiality Audit*,  
This document looks specifically at patient confidentiality within the pharmacy setting. It identifies an audit tool enabling pharmacists to look constructively at current data protection practice. The document also identifies how realistic, measurable change can be approached.

http://www.rpsgb.org.uk/pdfs/confidentiality.pdf

The Royal Pharmaceutical Society of Great Britain (RPSGB) also produces a fact sheet with guidance on Confidentiality, Data Protection and disclosure of patient information. This is currently being updated but will become available on their website.

Web Site – Scottish Government Open Learning Workbook  
This web site contains a wealth of information on the Freedom of Information (Scotland) Act 2002.

http://www.scotland.gov.uk/Publications/2004/02/18961/33482

Part 1 - Patient Confidentiality  
The following section covers the general issue of patient confidentiality.  
Accurate and secure information is an essential part of patient health care. Therefore it is important that all health professionals and others working for NHSScotland protect the confidentiality of patient information according to best practice and the law. Information given in confidence should not be disclosed in a form that might identify a patient without their consent (see Part 2 of this section).

The basic principles are quite straightforward:

- Patient information should be recorded accurately
Patient information should be physically secure
Guidance should be followed before disclosing patient information
Best practice should be followed in respect of access to all patient information
Information should be anonymised where possible

In addition, the RPSGB has set a number of standards with regards patient confidentiality. They include:
- The duty of confidentiality - patients have a right to expect that any information obtained about them is kept confidential and only used for the purposes for which it was given. This extends to the whole pharmacy team involved in the care of patients.
- Keeping information confidential - taking all reasonable steps to prevent disclosure or unauthorised access to confidential or patient identifiable information. Even accidental disclosure of information constitutes a breach of confidentiality.

**What is patient identifiable information?**

The definition of Patient Identifiable Information given in the NHS Code of Practice is:
- The patient’s name
- The patient’s address
- The patient’s full postcode
- The patient’s date of birth
- The patient’s CHI number
- A picture, photograph, video, audio-tape or other images

The CHI number indicates date of birth and sex so it should only be disclosed for health care purposes outside the NHS with the patient’s consent.

**Question 1 - What pharmacy specific material would you consider patient identifiable?**

<table>
<thead>
<tr>
<th>Material</th>
<th>Tick</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient Medication Records</td>
<td></td>
</tr>
<tr>
<td>Prescriptions</td>
<td></td>
</tr>
<tr>
<td>Receipts</td>
<td></td>
</tr>
<tr>
<td>Owings slips</td>
<td></td>
</tr>
<tr>
<td>Spare or discarded labels</td>
<td></td>
</tr>
<tr>
<td>CD Registers</td>
<td></td>
</tr>
<tr>
<td>Private Prescription Registers</td>
<td></td>
</tr>
<tr>
<td>CCTV Images</td>
<td></td>
</tr>
<tr>
<td>All of the above</td>
<td></td>
</tr>
</tbody>
</table>
All records, registers, prescriptions and other sources of confidential information should be stored securely and kept out of sight of patients, members of the public and any other person who should not have access to them.

Any sources of patient identifiable information must also be disposed of in a manner that prevents the information being seen by, or available to, non-authorised persons. Ways of disposing of patient identifiable information include shredding documentation or deleting information using a permanent marker. Section 2 of the Toolkit covers disposing of patient data held on your computer system.

Think about situations in the pharmacy when you or a member of your staff might handle patient identifiable information.

Examples may include:

- when receiving a prescription at the medicines counter
- prescription collection and delivery services
- a patient / patients representative request to collect a prescription or owing
- a query to a GP practice about a patient’s prescription
- handling of prescriptions in the dispensary
- discarding prescription stationery e.g. repeat ordering slips, void prescriptions, the right hand side of a prescription form
- storing prescriptions in the dispensary, either prior to sending to PSD or for owings, instalment dispensing etc.

**Question 2 – What procedures do you have in place for handling patient identifiable information?** Tick the standard you currently meet.

<table>
<thead>
<tr>
<th>Standard - Poor</th>
<th>Standard - Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No procedures in place</td>
<td>Procedures in place for when and how patient identifiable information is used (or destroyed)</td>
<td>Individuals asking for patient identifiable information are being positively identified as being entitled to that information Patient identifying information is removed from documents unless there is a specific need for it</td>
</tr>
</tbody>
</table>

From this exercise and the example scenarios consider any requirements that you can identify for the need for procedures to handle patient identifiable information in your pharmacy and put in place plans to address any gaps.

Best practice should be followed for all forms of patient information whether this be paper records, electronic data, e-mails, surface mail or even conversations or phone calls which can be overheard.
Question 3 – Do you have identified standards or protocols that you use when discussing patient information in your pharmacy? Are your staff aware of them? Tick the standard you currently meet?

Consider how all forms of patient information (paper records, electronic data, e-mails, post, conversations and phone calls) are handled in your pharmacy.

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard - Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discussed openly within the pharmacy</td>
<td>Discussed in private areas only but can be overheard</td>
<td>Avoidance of discussion of patient information where it can be overheard</td>
</tr>
</tbody>
</table>

From this exercise consider whether you require to develop any specific protocols for discussing patient information in your pharmacy for staff and detail plans to address any gaps.

You may also wish to consider the handling of patient identifiable information when developing and reviewing any Standard Operating Procedures (SOPs) in your pharmacy. Areas to consider include:

- who has access to patient information and in what circumstances
- how information is processed, used and stored

**Keeping information confidential with the pharmacy team**

All employees, students, volunteers and contractors and their staff must comply with the *Code of Practice on Protecting Patient Confidentiality*. Failure to do so may result in a professional, disciplinary or civil legal proceeding.

This means that all members of the pharmacy team should be aware of the requirements of the Code and know where to seek support, further information and training and be able to demonstrate that they are making every reasonable effort to comply with the relevant standards.

Training on the code and the importance of patient confidentiality should be included in any induction procedures for new staff and as part of any ongoing training for existing or recently promoted staff. Many of the organisations from whom you purchase training materials will cover patient confidentiality issues.

You may wish to check the content of any staff induction programmes or training materials provided to establish whether they provide training on confidentiality. Staff contracts often include a patient confidentiality agreement. In addition, some pharmacies may have a code of conduct for patient confidentiality.

**Question 4 – Do you have staff induction procedures and training programmes, contractual requirements or a code of conduct that cover the issues of protecting patient confidentiality for full, part-time or temporary staff who work in or on behalf of your pharmacy? Tick the standard you currently meet?**
<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard - Average</th>
<th>Standard - Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No mention of confidentiality and security requirements in induction for most staff. No training provided.</td>
<td>Basic requirements outlined as part of induction process for all staff</td>
<td>Understanding of the requirements of confidentiality and security is enhanced by training and comprehension checked</td>
</tr>
<tr>
<td>No confidentiality requirements included in staff contracts</td>
<td>Confidentiality requirements included for some staff in their contract</td>
<td>Confidentiality requirements included in the contracts for all staff</td>
</tr>
<tr>
<td>No code of conduct exists or staff are not generally aware of it</td>
<td>Code of conduct exists and all staff are aware of it</td>
<td>Code of conduct regularly reviewed and updated</td>
</tr>
</tbody>
</table>

From this exercise consider any requirements that you can identify in your pharmacy for new or existing staff to improve their awareness on protecting patient confidentiality and detail plans to address any gaps.

You might want to carry out a training needs assessment to identify any gaps in knowledge in order to establish what training requirements your staff have in this area.

**Part 2 – Patient Consent**

Patients have different values; what is very sensitive and important to one person can be causally viewed by another. The Code of Practice states that all health professionals and staff must, amongst other things:

- obtains a person’s informed consent before using their data in ways that do not directly contribute to patient care
- respect and record patients’ decisions to agree to or restrict the use of information regarding them
- communicate effectively with patients with regards consent to share information and the possible consequences of any actions
- answer queries or questions related to sharing of information

Patients must be informed about the use of their information and their consent obtained before their information is used in ways that do not directly contribute to or support the delivery or planning of their health care and this should be an ongoing process, not just a single event.

Patient consent should also be informed (i.e. they understand the implications of their actions) and freely given. It can be written or verbal and patients can change their mind about consent at any time.

Consent can be implied (when a patient has been given information about a disclosure, has been presented with the opportunity to object and then accepts the disclosure / service without giving an objection) or explicit (when they actively
express consent). Obviously explicit consent is best practice, particularly as we move toward patients active involvement in decisions about their care.

A patients' decisions to agree or disagree with the disclosure of information should be recorded. In addition, any implications of an agreement or non-agreement to the disclosure of information by patients should be effectively communicated.

The Code of practice also states that requirements for consent should be considered against the following criteria:

- Legal requirement – in some circumstances the law requires clinicians to disclose information irrespective of the patient’s view (although the Data Protection Act requires the patient is told about the disclosure).
- To protect patients’ vital interests – where a child or vulnerable adult may be in need of protection or at risk of death or serious harm.
- In the interests of the public – for the production of health planning statistics or disclosing information to the Police to help prevent or detect serious crime (both the Data Protection Act and professional standards allow for this).
- Children and adults who are unable to consent – in most cases someone (either a guardian or parent) is entitled to give consent on their behalf.

The RPSGB guidance on patient consent describes the following steps to obtaining consent:

- Provide sufficient information to enable patients to make an informed decision, including the reason, the benefits and risks, the implications of not providing consent and any alternatives that may be available
- Present information to patients in a way that they will understand and give them time to absorb the information and come back for questions if required.
- Respond to any questions openly and honesty so as not to mislead the patient into giving consent
- Confirm their understanding of the information provided.

It goes on to say that the person treating the patient should be the person who seeks consent. Therefore, in community pharmacy, it should be the pharmacist, although there may be times when it is appropriate to delegate this to another member of staff e.g. partaking in a prescription collection or delivery service.

As before the process of obtaining consent, where it is required, should be included in any SOPs for pharmacy services. Areas to consider include:

- Activities within the pharmacy that may require consent
- Activities that require the pharmacist to consent the patient and those that may be delegated to another member of staff
- The information that should be provided
- The type of consent required e.g. implied, written, verbal etc.

The RPSGB guidance goes on to explore the presence of a third person (e.g. a pre-registration student), adults and children without capacity to consent, refusal to consent and emergencies.
Of course, the key to successful patient consent is the quality of the information provided to patients to help them make informed decisions about the use of any data relating to them or their care. Including an appropriate section in your practice leaflet is a very practical way of doing this.

In addition the Health Rights Information Scotland leaflet ‘Confidentiality – it’s your Right’ is another useful tool to provide patients with information on confidentiality and consent. Copies are available from your local NHS Board or from the HRIS website:


**Part 3 - Maintaining information and retaining records**

Both the Data Protection Act and the Code of Practice states that organisations should use the **MINIMUM** amount of information on a **need to know** basis and to retain it only for as long as is needed for the purpose for which it was originally collected. Section one of the Toolkit outlines good practice in maintaining records.

The Data Protection Act does not specify how long Pharmacy Patient Medication Records should be kept for but advises that information should be kept no longer than necessary. The NHSScotland website on patient confidentiality contains some advice and guidance on the retention periods for health records but not specifically for community pharmacy.

The RPSGB advise that each pharmacy should have their own retention policy with a timescale dependent on the importance of the data or whether there is a legal obligation to retain the information.

**Question 5 – Do you have a data retention policy for your PMR data? If not think about what parameters you might want to put in place?**

You may wish to think how you use the data held on your PMR. For example, if the data is being used to help in the clinical assessment during the dispensing of an acute prescription then there may be no useful purpose in keeping a record indefinitely. However, if the patient regularly brings in prescriptions then there is a greater benefit in keeping a complete record of all acute and repeat prescribing events for a longer time period. In this situation there is a case for keeping the record for at least as long as the patient remains a regular patient and for a period of time after.

If your PMR record is the only record of a medicine supplied and dispensed then good practice states that a record should be retained for at least 13 years for an adult patient, or until a child or young person reaches 25 years of age, unless the information could be obtained in a different way. If a patient dies the record should be retained for three years after their death.

If the PMR constitutes the record of POMs and CDs supplied instead of a paper CD register, then it needs to be kept for 2 years after the entry. If the PMR is used for records of private prescriptions, with no hard copy register, then 7 years is needed for VAT purposes.
Part 4 – Disclosure of Information

This part deals more specifically with disclosure of patient information. The Data Protection Act requires any organisation that holds data about patients to be able to process the information it holds safely, including obtaining, recording, holding, using and disclosing information. In order to oversee this, each organisation should have a data controller who is ultimately responsible for the processing of any data and for the actions of any other staff involved. In addition, patients need to be informed of the identity of the data controller and the purposes to which their data will be put.

The definition of data controller is given as ‘the legal “person” (limited company, single handed practitioner, partnership etc.) that determines how, and for what purposes, information from patients is collected’.

Community pharmacy contractors are required under statute to notify the Information Commissioner’s Office (ICO) of certain details about their processing of personal information. These details are used by the Information Commissioner to make an entry describing the processing in the Register of Data Controllers that is available to the public for inspection.

The principal purpose of having notification and the public register is transparency and openness. It is a basic principle of data protection that the public should know (or should be able to find out) who is carrying out the processing of personal information as well as other details about the processing (such as for what reason it is being carried out).

It is not, however, intended (nor is it practicable) that the register should contain very detailed information about a data controller’s processing. The aim is to keep the content at a general level, with sufficient detail to give an overall picture of the processing. More detail is only necessary to satisfy specific statutory requirements or where there is particular sensitivity.

Question 6 – who is the named data controller for your pharmacy?

Name of data controller:

Think about how you might make patients aware of the data controller for your pharmacy. For example, you could include a section in your practice leaflet naming the data controller or explaining how to make a request to them.

The NHS has a duty to make people aware of the way it will use their data whether it is related to the provision of direct health care such as between members of the healthcare team or health organisations or for less obvious uses such as planning, clinical governance, payment and clinical audits. As far as possible this information should be anonymised.

For example look at the back of a GP10 or CP2 prescription form; you will notice that it informs patients of the use of their data in exemptions checks or for anonymised data collections for use by the NHS.

Patients can be given information about the use of their data in a range of ways, for example, by talking to them or providing leaflets or other materials (consider the
need for translations). It is also important to check that patients have received and understood what and when information is recorded and how it is disclosed.

Think about the uses that you, your local GP practice and the NHS may make of patient data. You might want to ask your local GP practice how it informs people of the use of any data and think about any actions you may need to take.

**Question 7 – do you have documentation available on how patient information is used in your pharmacy?** Tick the standard you currently meet.

<table>
<thead>
<tr>
<th>Standard – Poor</th>
<th>Standard - Average</th>
<th>Standard – Excellent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No information or simple posters and leaflets in waiting area</td>
<td>An active campaign in place to promote understanding of NHS information use</td>
<td>An active campaign including arrangements for patients with special or different needs</td>
</tr>
</tbody>
</table>

From this exercise consider any requirements that you can identify in your pharmacy for informing patients on how information that you keep will be used. For example, you might use your practice leaflet to explain how you use patient data e.g. for maintaining a patient record on your PMR system or the HRIS Patient Confidentiality leaflet to raise awareness.

You may also wish to consider the disclosure of patient information when developing and reviewing any Standard Operating Procedures (SOPs) in your pharmacy.

Your Freedom of Information Publication Scheme demonstrates your commitment to make information available and also details how and where that information is available.

**Question 8 – Is your Freedom of Information Publication Scheme up to date and accessible in your pharmacy?**

Community Pharmacy Scotland provided a model publication scheme for community pharmacy contractors to use in response to any requests about information regarding NHS pharmaceutical services. The model publication scheme can be downloaded from the CPS web site.
**ACTION LIST**

Having completed sections 1, 2 and 3 you may have some further actions to take forward from the exercises you have completed. Please record them here and then you can track your progress against each one and mark it completed as appropriate.

<table>
<thead>
<tr>
<th>SECTION</th>
<th>ACTIONS</th>
<th>COMPLETED BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECTION ONE: UPDATING PMR RECORDS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SECTION TWO: DATA BACKUPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SECTION THREE: DATA PROTECTION &amp; PATIENT CONFIDENTIALITY</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX 1 N3 & Anti-Virus

What is N3?

N3 is the national network for the NHS. It provides reliable IT infrastructure, world class networking services and sufficient, secure connectivity and broadband capacity to meet current and future NHS IT needs.

N3 will link all NHS organisations in Scotland, providing a reliable service to enable secure transmission of clinical data.

What are the benefits of N3?

N3 underpins and enables the delivery of IT systems and services for the NHS. The N3 network provides the essential technical infrastructure through which the benefits to patients and staff from IT systems and services will be fully realised and sustained in the future.

N3 provides the ability for Pharmacies to communicate with NHS Scotland and participate in current or evolving eHealth initiatives. Put in basic terms, N3 is simply a network allowing data to be transferred securely from one organisation to another.

What services does N3 deliver?

N3 does not directly deliver any services; it is the services that connect to N3 and utilise the network that will deliver benefits to Pharmacies. The following list provides some examples of current and potential future services, but is by no means exhaustive:

- NHS Mail – access to an NHS email address for life, providing the ability to communicate securely. Further information on NHS Mail and its use can be found on the community pharmacy website. There is a quick guide included as an Appendix to the Toolkit (see Appendix 4).
- National CHI system – a CHI number being present on all patient communication has been a mandatory requirement for a number of months now. N3 will provide the links to CHI in order for this to be achieved.
- Broadband Internet access – N3 provides internet access allowing internet sites and resources to be utilised (e.g. NES Education Portal). Also enables access to local health board Intranets.

Does N3 include a clinical system?

No. As stated above N3 is simply a computer network which transmits data.
Symantec Anti-Virus Software

Your anti-virus (A/V) software should automatically update itself, or, in the case of pharmacy multiples the updates are handled at Head Office level. It is possible, however, that the automatic element of your A/V software is not active. If this is the case, you should update your anti-virus software manually ideally daily but at least once a week. The longer you leave between updates, the higher the risk of a virus infecting your computer.

Your computer may show you a dialog box telling you that your virus definition files are out of date.

**Note:** Even if you do not see this dialog box it is important to check your anti-virus.

The above dialog box does not mean you have a virus. It only warns you that your virus definition information is a few days old. You need to run a manual live update to get the latest virus information/definitions.

**Running a Manual Live Update**

You access your anti-virus software from the task bar in the bottom right of the screen.

(If you cannot see many icons in this area, click the double-headed arrow to extend the bar)

1. Double click the A/V icon, which looks like a shield.
This opens the Symantec AntiVirus screen.

2. Check the **date** to the left of the LiveUpdate button. If it is more than 1 week old, complete the following procedure.

3. Click the **LiveUpdate** button.

![LiveUpdate dialog box](image)

This opens the LiveUpdate dialog box.

4. Click the **Next** button.
A LiveUpdate begins. The bold blue bar(s) along the middle of the screen show the progress of the LiveUpdate. (There may be 2 bars)

You will see the finish screen. It displays a big green tick showing your update has been successful.

5. Click the Finish button to complete the update procedure.

6. Allow the computer time to update any computer files and change the date on the screen beside the LiveUpdate button.

   Note: The new date given may not be today’s date as virus definitions are not released every day.
APPENDIX 2: BACK-UP LOG

Pharmacy Name: _____________________  Staff members: _____________________
                                    _____________________  _____________________

Week beginning: _____________________

<table>
<thead>
<tr>
<th>Date</th>
<th>Tape</th>
<th>Auto/Manual</th>
<th>Time</th>
<th>Status</th>
<th>Comments</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX 3 USEFUL WEB SITES

Your PC has the ability to save websites as 'Favourites' and in addition to any you already have stored you may wish to add the following:

<table>
<thead>
<tr>
<th>Website</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.communitypharmacy.scot.nhs.uk">www.communitypharmacy.scot.nhs.uk</a></td>
<td>Community pharmacy contract website</td>
</tr>
<tr>
<td><a href="http://www.communitypharmacyscotland.org.uk">www.communitypharmacyscotland.org.uk</a></td>
<td>Community Pharmacy Scotland website</td>
</tr>
<tr>
<td><a href="http://www.nes.scot.nhs.uk/pharmacy">www.nes.scot.nhs.uk/pharmacy</a></td>
<td>NHS Education Scotland Pharmacy link</td>
</tr>
<tr>
<td><a href="http://www.elib.scot.nhs.uk">www.elib.scot.nhs.uk</a></td>
<td>NHS Scotland eLibrary portal</td>
</tr>
<tr>
<td><a href="http://www.show.scot.nhs.uk">www.show.scot.nhs.uk</a></td>
<td>Online NHS health Information</td>
</tr>
<tr>
<td><a href="http://www.sehd.scot.nhs.uk">www.sehd.scot.nhs.uk</a></td>
<td>Publications from the Scottish Government</td>
</tr>
<tr>
<td><a href="http://www.psd.scot.nhs.uk">www.psd.scot.nhs.uk</a></td>
<td>Practitioner Services Division of NSS</td>
</tr>
<tr>
<td><a href="http://www.isdscotland.org">www.isdscotland.org</a></td>
<td>Information Statistics Division of NSS</td>
</tr>
<tr>
<td><a href="http://www.cfs.scot.nhs.uk">www.cfs.scot.nhs.uk</a></td>
<td>Counter Fraud Services Scotland</td>
</tr>
<tr>
<td><a href="http://www.rpsgb.org.uk">www.rpsgb.org.uk</a></td>
<td>Royal Pharmaceutical Society of Great Britain</td>
</tr>
<tr>
<td><a href="http://www.nhs.net">www.nhs.net</a></td>
<td>NHSmail website</td>
</tr>
<tr>
<td><a href="http://www.bma.org.uk">www.bma.org.uk</a></td>
<td>British Medical Association</td>
</tr>
<tr>
<td><a href="http://www.gdc-uk.org">www.gdc-uk.org</a></td>
<td>General Dental Council</td>
</tr>
<tr>
<td><a href="http://www.hmrc.gov.uk">www.hmrc.gov.uk</a></td>
<td>HM Revenue &amp; Customs</td>
</tr>
<tr>
<td><a href="http://www.hse.gov.uk">www.hse.gov.uk</a></td>
<td>Health &amp; Safety Executive</td>
</tr>
<tr>
<td><a href="http://www.bbc.co.uk">www.bbc.co.uk</a></td>
<td>Access to latest news, weather etc.</td>
</tr>
<tr>
<td><a href="http://www.google.co.uk">www.google.co.uk</a></td>
<td>Search Engine</td>
</tr>
<tr>
<td><a href="http://www.trafficscotland.org">www.trafficscotland.org</a></td>
<td>Real time traffic information for Scotland</td>
</tr>
<tr>
<td><a href="http://www.multimap.com">www.multimap.com</a></td>
<td>Online maps</td>
</tr>
<tr>
<td>ACRONYMS:</td>
<td>-</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---</td>
</tr>
<tr>
<td>ADTC</td>
<td>Area Drug &amp; Therapeutics Committee</td>
</tr>
<tr>
<td>AHPs</td>
<td>Allied Healthcare Professionals</td>
</tr>
<tr>
<td>AMS</td>
<td>Acute Medication Service</td>
</tr>
<tr>
<td>CHD</td>
<td>Coronary Heart Disease</td>
</tr>
<tr>
<td>CHI</td>
<td>Community Health Index</td>
</tr>
<tr>
<td>CMS</td>
<td>Chronic Medication Service</td>
</tr>
<tr>
<td>CPD</td>
<td>Continuing Professional Development</td>
</tr>
<tr>
<td>CPS</td>
<td>Community Pharmacy Scotland</td>
</tr>
<tr>
<td>CSM</td>
<td>Committee on Safety of Medicines</td>
</tr>
<tr>
<td>CTO</td>
<td>Community Treatment Order</td>
</tr>
<tr>
<td>DCVP</td>
<td>Data Capture Validation and Pricing</td>
</tr>
<tr>
<td>ETP</td>
<td>Electronic Transmission of Prescriptions</td>
</tr>
<tr>
<td>ISD</td>
<td>Information &amp; Statistics Division</td>
</tr>
<tr>
<td>MAS</td>
<td>Minor Ailment Service</td>
</tr>
<tr>
<td>MCNs</td>
<td>Managed Clinical Networks</td>
</tr>
<tr>
<td>NSS</td>
<td>National Services Scotland</td>
</tr>
<tr>
<td>PIL</td>
<td>Patient Information Leaflet</td>
</tr>
<tr>
<td>PHS</td>
<td>Public Health Service</td>
</tr>
<tr>
<td>POM</td>
<td>Prescription Only Medicine</td>
</tr>
<tr>
<td>PRS</td>
<td>Patient Registration System</td>
</tr>
<tr>
<td>PSD</td>
<td>Practitioner Services Division</td>
</tr>
<tr>
<td>RPSGB</td>
<td>Royal Pharmaceutical Society of Great Britain</td>
</tr>
<tr>
<td>SG</td>
<td>Scottish Government</td>
</tr>
<tr>
<td>SMC</td>
<td>Scottish Medicines Consortium</td>
</tr>
<tr>
<td>UPN</td>
<td>Unique Prescription Number</td>
</tr>
</tbody>
</table>
Acknowledgements

Special thanks for their hard work and effort are due to all the Community Pharmacy IM&T Facilitators in developing this Toolkit and in particular to:

Delia Bryce, CP IM&T Facilitator, NHS Lanarkshire
Laura Gill, CP IM&T Facilitator, NHS Ayrshire & Arran
Catriona Macdonald, CP IM&T Facilitator, NHS Tayside
Rowen Paton, CP IM&T Facilitator, NHS Greater Glasgow & Clyde
Catherine Scoular, CP IM&T Facilitator, NHS Greater Glasgow & Clyde