Pharmacy Practice in England: How the necessity of Legal and Regulatory compliance shapes the Community Pharmacy Practice, Network, Communications and Storage of Customer Data

GIAC Security Essentials Certification (GSEC) Practical Assignment (v1.4c)
Option 1 Research Paper

Natalie Moult

December 9, 2004

Abstract

Pharmacies in England, dispensing medicines to the general public, are increasingly holding more patient data (PMRs – Patient Medication Records) within their own electronic infrastructure to aid their practice and improve quality of service.

This paper will discuss the security issues faced for data protection when designing pharmacy practices and IT infrastructure, in light of legal considerations (UK and EU) and the imminent introduction of Electronic Transmission of Prescriptions (ETP) over the National Health Service (NHS) WAN, "N3" (new National Network) and its implications.

Disclaimer

This paper does not constitute legal advice. Always seek qualified legal counsel when dealing with the processing of sensitive data.

Table of Contents

1.0 Introduction

Pharmacies were one of the forerunners within the medical profession in England, for the electronic capture of patient information, the first computer-based systems being available in the late 1970s[1]. This was initially driven by label printing requirements for dispensed medicines, but latterly by the drive to provide improved clinical services[2].

Initially these pharmacy computer systems were standalone, non-networked entities with each pharmacy creating, owning and maintaining their customer's records. The security risks posed, when the only method of accessing the data could be from the computer itself, were far lower than those experienced today.

These days, traditionally paper-based pharmacy resources such as the British National Formulary (BNF), are available in electronic form with updates available from the Internet. With the necessity for regular drug updates and the advent of electronic ordering and references, the number of discrete pharmacy systems is dwindling.

As the instances of networked systems increase, so do the risks threatening those systems.

We will first look at the data that pharmacies may be required to hold in order to achieve their remit. We will then analyse the legal issues that surround this data, moving onto a discussion of the NHS's NPfIT (National Programme for Information Technology) project, the future plans for electronic transmission of prescriptions and the government requirements for conformance for inclusion. Finally we will explore the security measures necessary for compliance.

[1] PMRs – Distance Learning Course; CPPE (Mary Snell)
[2] As (1) above – Research cited from University of Bath

2.0 Patient Medication Records

2.1 Data Types

To comply with the Royal Pharmaceutical Society Guidelines, dispensing pharmacies will require to utilise the following information during dispensing transactions :

Patient Details	Name (Surname, given name & title)
	Address, including postcode
	Telephone number
	Sex
	Date of Birth
	NHS Number
	Name of residential /nursing home (where appropriate)
	GP's (General Practitioner's) name
Prescriber Details	Name
	ID number
	Practice Name
	Practice contact details
Dispensed Medicine detail	Name
	Form
	Strength
	Quantity & unit of measure
	Dosage regimen
	Date of dispensing
	Batch number
	Expiry date

Table 1 : ENV 13607 minimum PMR requirements[3]

2.2 PMR Use

The primary use of PMRs is for printing labels for dispensed medicines, they are also used within the pharmacy, by the pharmacist to enhance the clinical customer service.

2.3 Data Classification

Under the Data Protection Act 1998, Part I, Preliminary, section 2, (e) defines any information consisting of data as to a persons physical or mental health or condition as sensitive personal data. PMRs should therefore be considered as confidential.

[3] Taken from PMRs – Distance Learning Course; CPPE (Mary Snell)

2.4 The Importance of CIA

When working with PMRs, the three tenets of information security are applied as follows :

2.4.1 Confidentiality

The data held on patients must be considered confidential and should be treated as such, for reasons that will be discussed in the section 3.0.

2.4.2 Integrity

The integrity of the PMRs is of utmost importance. Many PMR systems are used to identify drug interactions from the patient's dispensed medicine history, the function of this is to provide warnings to the pharmacist that a drug interaction exists, the pharmacist can then act accordingly. If the record becomes corrupted, for example by a dispensed drug being deleted from the patient's history, a potentially fatal interaction may pass unnoticed. This could leave the pharmacist liable in a case of negligence.

2.4.3 Availability

The availability of PMRs is essential in the day to day operation of the pharmacy for repeat prescriptions and drug interactions, amongst other procedures.

3.0 UK & EU Law and Professional Regulations

Pharmacies in England are subject to a range of legal and regulatory controls with regard to the privileged data they hold on their customers. The legal responsibilities fall under two broad banners; IT related and practice related. We will touch briefly upon the practice related law where it intersects with the IT regulations or affects security, otherwise we will focus upon the legislation that influences (or should influence) the computing systems for pharmacy.

3.1 The Data Protection Act 1998 (DPA)

The DPA came into force on 1st March 2000, superseding the Data Protection Act 1984. It implements the EC Data Protection Directive 95/46/EC.

The 7th principle states that :

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."[4] (Please see Appendix B for interpretation of the 7th principle).

The DPA therefore clearly stipulates that pharmacies are obliged, by law, to exercise due diligence with regard to patient data, and security measures must be taken to prevent the loss of, or unauthorised access to those records.

3.2 The Human Rights Act 1998 (HRA)

The HRA came into force in October 2000 and replaces the British common law of confidence with regard to the use of data. "The general rule is that information given or received in confidence for one purpose may not be used for another purpose or passed to anyone without the consent of the person who gave the confidential information."[5]

3.3 The Royal Pharmaceutical Society of Great Britain (RPSGB)

The RPSGB is the regulatory and professional body for pharmacists in England. The primary objective is to lead, regulate and develop the pharmacy profession.[6] In this capacity the RPSGB provide guidance and training for all aspects of the pharmacy profession, including the use of PMRs. The RPSGB builds upon the baselines created by legislation, therefore ensuring that the minimum standards are met.

3.4 The Caldicott Report

The Caldicott Committee was set up in 1996 "to review the transfer of all patient-identifiable information from NHS organisations to other NHS or non-NHS bodies for purposes other than direct care, medical research or where there is a statutory requirement for information."[7]

The report, issued in December 1997, made a number of recommendations, of which pharmacies in contract with the NHS are required to adopt, including:

- Appointment of a "Caldicott Guardian" who should be a senior health official within the organisation
- Ensuring mechanisms are in place for physical security, security awareness, security management and policies
- Effective password protection

[4] DPA, Schedule 1, URL: http://www.hmso.gov.uk/acts/acts1998/80029--l.htm#sch1
[5] PMRs – Distance Learning Course; CPPE (Mary Snell)
[6] RPSGB URL: http://www.rpsgb.org.uk
[7] The Caldicott Report, URL: http://www.publications.doh.gov.uk/ipu/confiden/report/intro.htm

The National Confidentiality and Security Advisory Body has been formed to support Caldicott Guardians in their role as information guardians within their organisations.[8]

3.5 The Consumer Protection Act 1987 (CPA)

The Consumer Protection Act has an influence on the amount of time backups of PMRs are held. For product liability reasons, it is recommended by the RPSGB that records be held in archive for 13 years.

4.0 NHS Future Pharmacy Strategy

4.1 Electronic Transmission of Prescriptions (ETP)

In September 2000, the Department of Health published its vision for the future of pharmacy working with the NHS.

"By 2004, electronic prescriptions will be routine in the community as well as hospitals. Transfer of prescription data between GPs, pharmacies and the Prescription Pricing Authority will be carried out electronically, using the NHSNet, in the large majority of cases by 2008, or even earlier."[9]

Whilst we have not yet seen the envisaged routine use of electronic prescriptions in the community, work is currently underway to develop the N3 WAN (successor to the existing NHSnet) across the UK, and many community pharmacies are in discussions with NPfIT (the National Programme for Information Technology in the NHS) regarding their connection to the NHS infrastructure and subsequent use of ETP.

Following the successful completion of three pilot implementations (completed June 2003), where the electronic transmission of prescriptions was proved to be viable whilst maintaining data integrity and confidentiality, NPfIT aims to start introducing the use of ETP nationally in conjunction with pharmacies from January 2005.

Detailed information regarding NPfIT ETP compliance are considered commercially sensitive and therefore cannot be shared within this paper, however it is clear that the main areas that will need to be assessed for suitability and conformance are:-

- Dispensing applications
- Pharmacy network
- Access Control
- Physical Security

[8] DoH, URL: http://www.publications.doh.gov.uk/ipu/whatnew/newadvis.htm
[9] Section 2.16 – Pharmacy in the Future, Department of Health, Sept 2000

4.2 Other Future Pharmacy Developments

The Framework for a New Community Pharmacy Contract, released in conjunction with Vision for Pharmacy in the New NHS by the Department of Health (July 2003) proposes additional services other than dispensing medicines (defined as an essential service) that community pharmacies may provide in the future. These include supplementary prescribing (classed as an additional service) and medication use review (an enhanced service). These functions would conceivably require that the pharmacist has access to the patient's NHS medical records, which have until the present time been a separate entity to the pharmacy held PMR and have not been available to the pharmacist.

4.3 ETP & Enhanced Services Ramifications

The security requirements that ETP and the other future pharmacy functions enforce on the participating pharmacy are multi-layered. To perform the electronic roles the pharmacy will need to be connected to the N3 backbone; this introduces a number of requirements including network security, dispensing application compliance and access control.

5.0 Ensuring Compliance

Legal and industry regulations must be coupled with business requirements to form the policies for the pharmacy system. Standards and guidelines must then be written to support the policy in-line with the strategy and architecture (dictated by policy).

5.1 Defence In-Depth

To ensure that PMRs stay confidential, security must be applied in layers, a practice known as defence in-depth.

5.2 Data Protection Act registration

The DPA defines the person(s) who determine the purposes for which and the manner in which any personal data are, or are to be, processed as the Data Controller[10]. All Data Controllers must be registered with the Data Protection Commissioner in order to legally undertake this role, additionally, data may only be processed for the purpose registered with the Information Commissioner. Registration can be completed online at http://www.informationcommissioner.gov.uk/eventual.aspx?id=322

[10] DPA, URL: http://www.hmso.gov.uk/acts/acts1998/19980029.htm

5.3 Security Awareness

All pharmacy system users must understand the responsibility they hold when working with PMRs. All new staff should undergo security training, this could be part of the induction process and ongoing refresher sessions should be planned. Any person(s) whose role within the organisation involves them acting as a Data Controller (according to the DPA definition) should ensure they are registered at this point.

5.4 Policy

5.4.1 Acceptable Use

The creation of a policy to define how pharmacy systems will be used is a crucial aid to reinforcing the technical security measures and should be reinforced by awareness training - the human interface is often the flaw in an otherwise technically water-tight security solution.

The policy should be effective in clearly defining the responsibilities of the pharmacists and pharmacy assistants when handling this sensitive data, whilst removing some of the liability of the company in the case of a breach. The policy can be written specifically for the pharmacy users and the pharmacy system or it could be the Corporate Information Security and Acceptable Use policy.

The policy may include a clause mandating that all employees sign a Non-Disclosure Agreement (NDA) which specifically defines the rules on information disclosure by those accessing sensitive material.

A policy should not give direction on how the applications are used at an operational level, these details should be held in the relevant standards and guidelines which support the policy.

Sample policy statements of particular relevance to pharmacy systems are as follows:

- All users must authenticate to <the system> with their unique user ID, provided by <department> before performing any function
- Users will not create unauthorised internet connections (where modems are used)
- Users will not modify the system in any way other than those involved in the approved functions of their role
- Users will use passwords / passphrases which adhere to the <company> password policy (complying with the Caldicott report recommendations)
- Users will not discuss the content of PMRs or any other patient details within audible distance of unauthorised person(s)

There are many companies who specialise in DPA compliance measures who can supply policies which support a company's adherence to the DPA.

5.4.2 Technical

Technical policies should include:

- Network security
- Access control
- Password / passphrase policy
- Email policy
- Data classification policy
- Patching policy
- Backup Policy
- Pharmacy Computer configuration policy

5.5 Physical Security

Physical security of the pharmacy computers and printing apparatus should be addressed, as recommended by the Caldicott report. As a minimum, computers should be behind a barrier beyond which only staff are authorised to pass, for example the dispensing counter. If physical security is implemented well, the easiest access an unauthorised person has to the data is blocked.

5.6 Technical Design

5.6.1 Risk Assessment

A thorough risk assessment should be performed to identify vulnerabilities within an existing infrastructure, and remediation plans made to fill any gaps. Risk Assessment complying with BS7799-2 is advisable given that the current connection requirements for NHSnet are based upon partial BS7799 compliance, and it is therefore likely that NPfIT requirements will follow suit.

5.6.2 Network Infrastructure

As community pharmacies begin to make more use of the data they collect, there is an increasing need to allow computers used within the pharmacy onto a LAN, MAN or WAN (including the internet). This is most certainly the case with the new NHS backbone infrastructure and plans for community pharmacies to access patient medical records from the NHS.

The use of firewalls, Virtual LANs and Access Control Lists should all be considered when designing a pharmacy system. Network security is an important factor when accessing another organisation's systems, it is required that both parties become “trusted”. In order to achieve this, a baseline must be met, which will most certainly involve more than an ethernet connection and a valid IP address.

5.6.3 Pharmacy Workstations

The operating system must be hardened to provide only the functionality required and to remove any services, open ports and shared drives automatically configured with a standard installation. By hardening the build, the risk of infection by malware (malicious software) is reduced. This is particularly important when dealing with PMRs due to the need for data integrity (see section 2.4.2 above).

In addition to hardening, local anti-virus software should be installed, regular signature updates should be deployed and frequent scans scheduled. As a prerequisite for connection to the NHSnet, “All connected systems must be subject to up to date anti-Virus procedures and products”[11]

The patching policy for the organisation should govern the operating system and application patching required for the workstation and should be included in the regular operational maintenance process.

5.6.4 Access Control

Access to patient data must be controlled through the use of unique user ID’s where differing levels of authority and access rights can be granted to users based on role function within the pharmacy. Additionally, audit trails should be used where possible to log PMR creation, changes and deletions and the user who performed the function.

5.6.5 Data Storage

It is likely that more than one workstation will require access to the PMRs, therefore network attached storage will be necessary. The security of the storage device on which the data is held should be seen as high priority. Anti-virus software, local firewall, operating system hardening and encryption should be assessed for suitability.

[11] SyOP 8.2, URL: http://www.nhsia.nhs.uk/security/pages/syops/docs/coc.asp

5.6.6 Backups

Wherever backups are held, they must be protected. Encryption of the data is advisable especially if held on portable storage media such as compact discs. Offsite, secure storage should also be considered.
The RPSGB stipulate that backups should be made daily and advise that they are held offsite in a safe repository such as a bank.[12]

5.7 Security Operations

Security operations practices should include regular checks to ensure that adherence to policy continues. If the policies are written to help the pharmacy adhere to legislation and regulations, policy compliant practices are essential for the continued legal operation of the organisation.

6.0 Conclusion

In conclusion, the legal and regulatory requirements placed on pharmacies holding and processing patient records are clear in the message that the data is both sensitive and confidential, and should be treated accordingly. It is the responsibility of the organisation to ensure that the data is secured properly within their infrastructure and in transit. In fact the RPSGB state that the data should "be afforded the same degree of protection and vigilance that is given to money or to Controlled Drugs."

The main thrust is toward the confidentiality, integrity and availability of patient data. The Data Protection Act, Human Rights Act, Caldicott Report et al, all assert the rights of the customer as the data subject. The security solutions adopted by the organisation therefore need to support compliance by reducing the risks to the data whilst maintaining usability and availability for the pharmacy systems. A comprehensive information security policy, user training programme and technical architecture should be implemented to both satisfy the current provisions and to aid the transition when connecting to the NHS WAN, allowing for interoperability and compliance with minimum disruption.

[12] Guidance on Information Protection and Security, RPSGB, 2002

7.0 References

Snell, Mary. Patient Medication Records (Second Edition) – A Distance Learning Course for Pharmacists, Centre for Pharmacy Postgraduate Education, The University of Manchester, 2000

Watts, Geoff. "Electronic communication and health care: Paper prescriptions will soon be distinctly "last season"" BMJ 2004;328:1156 (15th May), doi:10.1136/bmj.328.7449.1156-a

Royal Pharmaceutical Society of Great Britain, Guidance on Information Protection and Security, PDF document, July 2002

Royal Pharmaceutical Society of Great Britain, Guidance on Information Protection and Security, PDF document, July 2002

Note: The two RPSGB documents above are currently being updated and will be published once completed on the RPSGB site
URL: http://www.rpsgb.org.uk/members/practice/framePractGuid.htm

The Royal Pharmaceutical Society of Great Britain
URL: http://www.rpsgb.org.uk

"The Data Protection Act 1998", The Stationary Office
URL: http://www.hmso.gov.uk/acts/acts1998/19980029.htm

Data Protection Act Guidance
URL: http://www.dti.gov.uk/SMD3/dp01-06d.htm

The Information Commissioner, "Data Protection Act 1998: Legal Guidance"
URL:
http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Data%20Protection%20Act%201998%20Legal%20Guidance.pdf

EU Directive 95/46 part 1
URL: http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

EU Directive 95/46 part 2
URL: http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf

Department of Health, "The Caldicott Committee:Report on the review of patient-identifiable information - December 1997
URL: http://www.publications.doh.gov.uk/ipu/confiden/report/intro.htm

Department of Health, "New Body to advise on Patient Confidentiality", March 2000
URL: http://www.publications.doh.gov.uk/ipu/whatnew/newadvis.htm

"The Human Rights Act 1998", The Stationary Office
URL: http://www.hmso.gov.uk/acts/acts1998/19980042.htm

"The Consumer Protection Act 1987 Commencement Order", The Stationary Office
URL: http://www.hmso.gov.uk/si/si1987/Uksi_19871680_en_1.htm

European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8
URL: http://europa.eu.int/comm/internal_market/privacy/law/treaty_en.htm

Department of Health, "Pharmacy in the Future – Implementing the NHS Plan: A Programme for Pharmacy in the National Health Service" September 2000
URL: http://www.dh.gov.uk/assetRoot/04/06/82/04/04068204.pdf

Department of Health, "A Vision for Pharmacy in the New NHS" July 2003
URL: http://www.dh.gov.uk/assetRoot/04/06/83/56/04068356.pdf

Department of Health, "Framework for a new Community Pharmacy Contract" July 2003
URL: http://www.dh.gov.uk/assetRoot/04/06/83/57/04068357.pdf

NPfIT "Electronic Transmission of Prescriptions" November 2004
URL: http://www.npfit.nhs.uk/programmes/etp/

NPfIT, "MakingITHappen" March 2004
URL:
http://www.npfit.nhs.uk/all_images_and_docs/making_IT_happen_0304.pdf

NPfIT, "MakingITWork – NpfIT Update" Issue 2, August 2004
URL:
http://www.npfit.nhs.uk/all_images_and_docs/making_IT_work_issue_2.pdf

NHS Information Authority "SyOP 8.2: Security Operating Procedure, Infrastructure – Code of Connection" 2002
URL: http://www.nhsia.nhs.uk/security/pages/syops/docs/coc.asp

Appendix A – A Crash Course in English Law

In order to abide by the Law with regard to computer-held information, it is important to understand the legal components.

An **Act of Parliament** is a law of the land. It must be passed through the Houses of Parliament as a Bill (and subsequently through the House of Lords). Once the MPs (Members of Parliament) and Peers (members of the House of Lords) have approved the bill, it will be sent to the Monarch for final approval. Once approved the bill becomes an Act of Parliament.

Statutory Instruments are known as subordinate or secondary legislation. They are made under an enabling Act (the primary legislation) and include regulations pertaining to the Act.

Common Law is non-statutory law, also know as the law of precedent, whereby previous judgements made in legal cases form the consensus over time (usually centuries) which eventually become common within the country's legal system.

Appendix B – Schedule I – The Data Protection Principles – Part II – Interpretation of the Principles in Part I – The Seventh Principle

The seventh principle

9. Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to-

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
(b) the nature of the data to be protected.

10. The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

11. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle-

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
(b) take reasonable steps to ensure compliance with those measures.

12. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless-

(a) the processing is carried out under a contract-
(i) which is made or evidenced in writing, and
(ii) under which the data processor is to act only on instructions from the data controller, and
(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.