

# NHS Information Governance: Pharmacy Contractor Workbook January 2010

## **Section 1: Overview**

	<b>Page</b>
Introduction to the NHS Requirements	2
How to use this Workbook	3
Quick Reference Guide to Actions Required	5

## **Section 2: Actions to Achieve Compliance**

114: Pharmacy IG Lead	6
115: Information Governance Policy	8
116: Contractual Confidentiality Clauses	10
117: Staff Awareness and Training	12
118: Completion of IGSoC	14
119: Monitoring Compliance with RA01 Terms	16
201: Confidentiality Code of Conduct	18
208: Mapping and Risk Assessing Information Flows	20
209: Offshore Data Transfers	22
212: Patient Consent	24
213: Patient Awareness	26
305: Ensuring Sufficient Access Controls to Information Systems	28
308: Exchange of Digital Information	30
316: Information Asset Register	32
317: Physical Security of Premises	34
318: Mobile Computing Systems	36
319: Business Continuity (requirement under development)	38
320: Incident Reporting	40

## **Section 3: Actions to Complete IGT Declaration and PCT Support**

Template Workplan (Appendix 1)	42
Guide to carrying out an IG Toolkit Assessment (Appendix 2)	43
Role of the PCT (Appendix 3)	46

## **Section 4: Background Material for Reference**

Confidentiality and the Law (Appendix 4)	47
Consent and the Law (Appendix 5)	51
Data Transfer Guidance (Appendix 6)	54
Guide to Mapping & Risk Assessing Information Flows	58
Glossary	63
Further Information and Support	64

**A range of downloadable templates and tools to support meeting the requirements can be accessed on the PSNC Website ([www.psn.org.uk/IG](http://www.psn.org.uk/IG)).**



**Royal  
Pharmaceutical  
Society**  
of Great Britain



**NHS Employers**

A part of the NHS Confederation  
working on behalf of the **NHS**



# Introduction to the NHS Information Governance Requirements

Information Governance ensures necessary safeguards for, and appropriate use of, patient and personal information. The widely reported high profile data losses by Government departments during 2007/08 increased the information governance priority within the NHS. The NHS Operating Framework 2009/10 introduced a requirement that by the end of 2009/10, all NHS providers (including community pharmacies) must be able to provide annual information governance assurances to their commissioners regarding the management of personal information within the provider organisation. These assurances are to be evidenced by the completion of the NHS Information Governance Toolkit (IGT), an online assessment tool, available at [www.igt.connectingforhealth.nhs.uk](http://www.igt.connectingforhealth.nhs.uk).

There are 18 information governance requirements for community pharmacy. The levels of achievement within each requirement range from zero to three. Completing this workbook will help you assess your current level of compliance and plan the steps needed to improve your pharmacy's level of compliance.

Information Governance assessments will need to be completed and submitted annually by the 31st March each year to demonstrate standards are being improved or maintained and will if necessary, need to be supported by a workplan which the PCT will monitor.

A small number of pharmacies connect to N3 directly rather than indirectly via a commercial 'network aggregator' such as IMS or Vialtus or via a corporate network. In addition to completing the Information Governance Toolkit, those pharmacies with a direct connection also need to ensure the NHS CFH Information Governance Statement of

Compliance (IGSoC) is completed and satisfied (Requirement 118). It is expected that this additional requirement to complete the IGSoC declaration will only apply to a handful of pharmacies.

## **Action by 31 March 2010**

All community pharmacies are required to complete an online baseline assessment against the requirements in the Information Governance Toolkit by 31 March 2010. This will provide a baseline for improvements to be carried out where necessary.

To do this, pharmacies will need to appoint an information governance Lead(s) who will complete the baseline assessment on the online Information Governance Toolkit. This is simply an honest evaluation of the pharmacy's current position in regards to each requirement. This workbook will support understanding the requirements and completing the assessment.

It is recognised that for many of the requirements, whilst pharmacies already have processes in place that ensure the secure handling of information, these may not be fully documented. This means that pharmacies won't have the evidence needed to meet Level 1 or 2 of the NHS requirements. It is therefore accepted that for many pharmacies some requirements will need to be baseline at 'Level 0'.

## **Action by 31 March 2011**

By 31 March 2011 community pharmacies will be expected to attain Level 2 against the pharmacy information governance requirements.

## **Funding Arrangements**

Agreement has been reached between the Department of Health (DH) and PSNC on the funding for the community pharmacy contractual framework

This resource has been produced jointly by the Pharmaceutical Services Negotiating Committee (PSNC) and the Royal Pharmaceutical Society of Great Britain (RPSGB) with the support of the Department of Health, NHS Employers and NHS Connecting for Health (CFH). Comments and suggestions on how to improve the guidance are welcomed and should be directed to [info@psnc.org.uk](mailto:info@psnc.org.uk)

Please note, this guidance is not intended to be construed as legal advice. If you believe that you require legal advice, please consult a solicitor or counsel.

for 2009/10. A proportion of excess margin will be used in 2009/10 to fund one-off infrastructure investments, to sustain the effective delivery of community pharmacy services. This includes progressing the information governance requirements.

*These requirements apply to England only. Different arrangements apply in Scotland, Wales and Northern Ireland.*

This workbook aims to provide guidance and support for pharmacies in meeting the NHS Information Governance requirements, completing the online Information Governance Toolkit and compiling appropriate evidence to demonstrate to a PCT compliance with the requirements.

In this workbook, for each requirement, there is a summary of the different levels of achievement, a list of the evidence required to demonstrate compliance, information about template resources and tools that are available to support meeting the requirements and space to make notes.

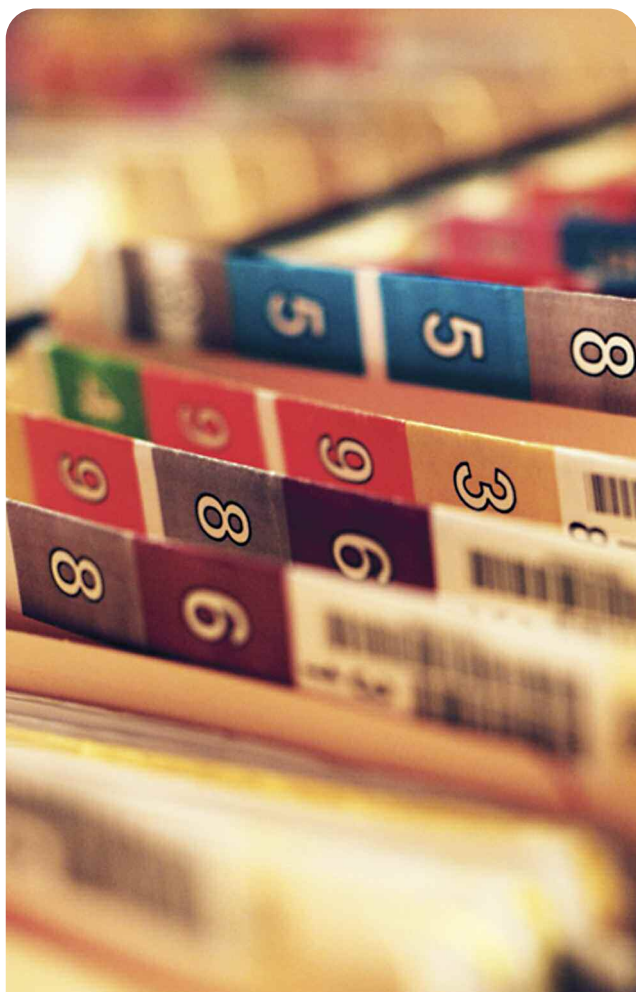
## **The Requirements**

Each NHS information governance requirement is numbered. Not all of the NHS requirements apply to pharmacies which is why the numbering of the pharmacy requirements is not sequential.

The levels of achievement within each requirement range from Level 0 to Level 3 where Level 0 is non-compliance and Level 3 is ongoing full-compliance. For a particular level to be achieved the pharmacy must also be able to demonstrate compliance with the previous levels, for example to achieve Level 2, the pharmacy must be able to show compliance with both Level 1 and Level 2 of the requirement.

## **Evidence of Compliance**

The evidence suggestions included in this workbook have been agreed by NHS Employers, DH, NHS CFH, PSNC and the RPSGB. This evidence would allow a pharmacy to demonstrate to their PCT compliance with the requirements; however the evidence suggested in this workbook is not prescriptive. Alternative pieces of evidence could serve the same purpose. For example, to support the requirement that all staff undertake appropriate training in Information Governance, a pharmacy may choose to develop their own in-house training



programme rather than use the nationally produced resources; likewise, rather than developing standard operating procedures (SOPs) a pharmacy may choose to document business process guidance or prepare policies. A pharmacy may also choose to use a different structure, content and format to the nationally provided templates and some of the process guidance and procedures may be encompassed in existing pharmacy internal governance documents which have a wider scope than that outlined in the national templates.

There is space in the workbook to note the evidence the pharmacy has, for example the location of SOPs and the name of the senior staff member that has approved the SOP. It may be helpful to create an 'Information Governance folder' to store your evidence for each requirement and as a central resource on Information Governance for staff to refer to; alternatively evidence could be stapled into the appropriate page in the workbook.

Care should be taken to ensure information which is either commercially sensitive or contains personal information is not shared with PCTs, for example the information asset register (316) or individual staff employment contracts (116). Further guidance on sharing information with PCTs can be found in Appendix 3.

### ***Multiples***

Where a pharmacy is part of a multiple chain, one possible approach is that the chain's Head Office will have assumed a leadership role in the delivery of Information Governance with many of the actions required to achieve compliance with the requirements undertaken by specialist staff based at the organisation's Head Office. In many cases local tailoring will also be required in order for each pharmacy to provide the necessary assurances to their PCT. Where supporting evidence is not

accessible locally, one approach could be for the Head Office to provide each of its sites with a supporting statement/ declaration as evidence of compliance. Examples of where this scenario is likely to occur include if the pharmacy information asset register is held centrally (316), where review of any data flows outside of the UK are undertaken centrally (209) and confirmation that personnel departments have ensured that staff and third party contractors have appropriate confidentiality clauses in contracts (116).

### ***Resources and Reference Material***

Templates and tools to support the completion of each requirement can be downloaded for local adaptation from the Pharmacy Information Governance Online Resource Centre ([www.psn.org.uk/IG](http://www.psn.org.uk/IG)).

Appendices 4 – 7 of this workbook contain background material which may be helpful for the Information Governance Lead's reference when working through the requirements. This background material does not form part of the requirements.

### ***Completing the Information Governance Toolkit / PCT Support***

Appendix 2 of this workbook includes a step-by-step guide to registering for access to the Information Governance Toolkit and submitting an assessment. Appendix 3 provides a briefing on the role of PCTs. PCTs will have visibility of Information Governance Toolkit Assessments undertaken by pharmacies in their area. This will enable the PCT to offer support where required, for example, if all pharmacies in their area are having difficulty with the same Information Governance Toolkit requirement(s).

The chart below is a quick reference guide to the key actions required to meet the pharmacy information governance requirements. Full details on the requirements can be found in the relevant section of this booklet. Templates can be downloaded from the PSNC website ([www.psn.org.uk/ig](http://www.psn.org.uk/ig)).

**Minimum Actions  
by 31st March 2010**

- Appoint IG Lead(s) (*Requirement 114*)
- IG Lead to take time to understand the requirements (*e.g. read this workbook*)
- Register for access to the online IG Toolkit (*Appendix 1*)
- Complete a Baseline Assessment on the IG Toolkit (*Appendix 1*)
- Create a Workplan (*NB: This is automatically generated as an output of making a submission to the online IGT*)

**Minimum Actions  
by 31st March 2011**

- Start working through the Pharmacy Workplan
- Ensure there are appropriate contractual clauses in staff and third party contracts (*Requirement 116 / Template 2*)
- Ensure staff are sufficiently trained in IG (*117 / Booklet "Introduction to Information Governance for Pharmacy Staff"*)
- Map, risk assess and put in place mitigating controls for data transfers (*Requirement 208 / Appendix 7*)
- Identify any overseas data transfers and put in place mitigating controls (*Requirement 209*)
- Create a patient information leaflet on how data is handled by the pharmacy (*Requirement 213 / Template 5*)
- Create an information asset register (*Requirement 316 / Template 6*)
- Risk assess physical security (*Requirement 317/Template 7*)
- Put in place an IG incident log (*Requirement 320 / Template 12*)
- Develop an IG policy (*Requirement 115/Template 1*)
- Develop a staff confidentiality code of conduct (*Requirement 201 / Appendix 3*)
- Develop one or more procedures that cover data transfer and safe havens (*Requirements 208 and 308 / Template 4*)
- Resources to support mobile computing (*Requirement 318 / Templates 8-10*)
- Develop an access control procedure (*Requirements 305 / Template 15*)
- Develop an IG incident management procedure (*Requirement 320 / Template 11*)
- Ensure policies, procedures and guidance materials are signed off by an appropriately senior staff member (*various*)
- Ensure staff have been informed of policies and procedures , where relevant (*various / template 14*)
- Put in place a system to monitor staff compliance with key requirements (*various / Template 13*)
- Complete Online IG Toolkit by 31st March 2011 and generate work plan

**NB: There are also requirements around business continuity (Requirement 319). Guidance on these will be published during 2010**

## Has responsibility for Information Governance been assigned to an appropriate member, or members, of staff?

This requires that named individuals take responsibility for co-ordinating, publicising and monitoring standards of information handling within the pharmacy and develop and implement an information governance workplan (also known as an implementation plan). The information governance Lead(s) also need(s) to ensure that Information Governance Toolkit assessments are submitted as required.

### Level 0

The pharmacy has not assigned Information Governance responsibilities.

### Level 1

The pharmacy has assigned responsibilities for Information Governance to a staff member or members who have been provided with appropriate training and support to carry out the role.

The pharmacy has put in place an information governance workplan (also known as an improvement plan) which documents both the current level of compliance with the NHS information governance requirements for the premises and the targets that have been identified to progress to the next level of compliance.

### Level 2

The pharmacy has implemented its information governance workplan to ensure a minimum of Level 2 compliance with each of the pharmacy requirements.

### Level 3

To achieve Level 3, the pharmacy must review its information governance arrangements annually.

## Hints and Tips

### Appointing an information governance Lead

- The pharmacy should consider the responsibilities of an information governance Lead and decide whether these can be met by one member of staff or whether the responsibilities should be shared between a number of staff. For contractors with multiple pharmacies, there may be a need to appoint staff both at Head Office and premises level. Those appointed do not need to be pharmacists but should have sufficient seniority and authority to ensure that any necessary changes in information handling within the pharmacy can be implemented and enforced.
- Ensuring confidentiality is already a key part of the clinical governance requirements in the pharmacy contractual framework. As a contractual framework requirement, all pharmacy premises must have an identifiable clinical governance lead. It is possible for the clinical governance lead to also act as the information governance Lead.
- There should be written assignment of information governance Lead responsibility. This could be through adding this to staff job descriptions or simply a written note of responsibility (for example, state who is responsible in the notes box).

### What training and support does the information governance Lead require?

- Information governance Lead(s) need to be sufficiently trained to undertake their key responsibilities. Training should cover data protection, security and confidentiality and Freedom of Information requirements. Where the information governance Lead is also the person responsible for data protection, confidentiality and Freedom of Information for the business, the training provided will need to be more extensive to ensure that the pharmacy complies with the law and guidance in these areas.
- **Thoroughly reading this workbook is sufficient to meet the Level 1 requirement for information governance Lead training.** However, if you are interested in learning more, one centrally provided training option is the Information Governance Training Tool provided by DH Informatics ([www.connectingforhealth.nhs.uk/igtrainingtool](http://www.connectingforhealth.nhs.uk/igtrainingtool)). The tool comprises a structured e-learning programme with Introductory, Foundation and Practitioner level modules covering all aspects of information governance. There is an introductory module on information governance for

pharmacy staff; this has been developed in conjunction with the PSNC and RPSGB. Other modules haven't been tailored to the pharmacy setting. To access the tool, users need to set up an account and, as part of the registration process, will be asked for their organisation's ODS Code (for pharmacies, this code begins with the letter F and can be found on the submission document used to send prescriptions to NHS Prescription Services each month). The resource can also be accessed without registering by taking the 'guest tour'. It is not necessary to have an email address to access or register for the tool.

- The information governance Lead should also have access to sufficient support within the pharmacy, for example if the information governance Lead is a non-

pharmacist, they should have access to a pharmacist for support with queries.

### Creating a Workplan

- Use this workbook to determine the pharmacy's current level of compliance. All pharmacies need to achieve Level 2 compliance by 31st March 2011. Appendix 1 contains a table which you might find useful to collate information on the pharmacy's current status.
- On completion of the Information Governance Toolkit, there is an option to print a workplan based on the information that has been input by the pharmacy. Note, the Information Governance Toolkit refers to this as an 'improvement plan'.

### Evidence

Level	Evidence Required	Resources Available	Yes/No
1	Written assignment of responsibility to staff member or members (e.g. note below)	-	
1	Written declaration on completion of information governance Lead training	Reading this workbook is sufficient. General training resources can be found on the Online Information Governance Training Tool.	
1	Copy of information governance workplan (improvement plan)	Template workplan (see Appendix 1). The Information Governance Toolkit creates a plan based on the information input by the pharmacy.	
2	Evidence of progress against the workplan/improvement plan	-	
3	Evidence of annual review (e.g. annual submission to the Information Governance Toolkit)	-	

### Notes

*Our information governance Lead(s) is/are .....*

*What training has the information governance Lead undertaken?*

## Does the pharmacy have an information governance policy that addresses the overall requirements of information governance?

Each pharmacy is required to have an information governance policy which is a high level statement of a pharmacy's intended approach to effectively managing information governance. The policy should outline the principles that underpin the policy, detail the pharmacy's information governance procedures and set out what is expected of pharmacy staff. The policy should reflect NHS information governance guidance and should be approved by a senior representative of the pharmacy.

### Level 0

The pharmacy does not have an Information Governance policy in place.

### Level 1

The pharmacy has reviewed, updated and drawn together all relevant policies to form a comprehensive Information Governance policy.

### Level 2

The pharmacy has an Information Governance policy that has been agreed by an appropriate senior staff member and conforms to national guidelines.

### Level 3

The policy has been made available to all pharmacy staff, including retail and administrative staff.

The policy is regularly reviewed and updated in the light of that review. Any amendments to the policy must be signed off by a senior representative of the pharmacy contractor.

## Hints and Tips

- Suggested key content of an information governance policy includes:
  - A section specifying why the policy is required – e.g. to safeguard the movement of personal data;
  - A summary of the procedures which underpin the policy to help ensure information will be handled securely and confidentially by the pharmacy (i.e. links to related SOPs);
  - A description of accountability and responsibility for the policy;
  - A process for monitoring the policy;
  - Pharmacy staff duties and responsibilities for information governance (maintaining confidentiality of data, ensuring secure storage of data, and being aware of situations where disclosure may be required); and
  - Actions to be taken if the policy is breached, e.g. sanctions against staff, remedial work on the part of those responsible for information governance procedure.
- A template policy can be downloaded from the online Information Governance Resource Centre. Each pharmacy will need to decide whether the template is sufficient for its needs and locally tailor the template as necessary.

**Evidence**

Level	Evidence Required	Resources Available	Yes/No
1	An Information Governance Policy	Template 1: Information Governance Policy	
2	Name of contractor representative that approved the Information Governance Policy (e.g. note below)	–	
3	Evidence that staff have been made aware of the policy	Template 14: Staff signature list	
3	Evidence of last review (e.g. note date of last review below)	–	

**Notes**

*The name of the senior staff member that approved the policy is .....*

*The policy was last reviewed on .....*

## Do all contracts (staff, contractor and third party) contain clauses that clearly identify responsibilities for confidentiality, data protection and security?

Pharmacies are required to ensure that all of their contracts with staff, locums and third parties who might have access to sensitive data (e.g. cleaners) contain clauses which clearly set out their responsibilities for ensuring and maintaining confidentiality, information security and data protection.

### Level 0

No staff contracts have clearly identified clauses addressing confidentiality, data protection and security.

### Level 1

The pharmacy has undertaken an audit of personnel records, and contractor and other third party contracts and determined how many of these have written contracts which contain clauses that identify responsibilities for confidentiality, data protection and information security, linked to disciplinary procedures.

The pharmacy has developed an action plan to update existing contracts, where necessary, and ensure all new contracts include compliance with information governance requirements as part of employment processes.

### Level 2

All pharmacy contracts for staff, contractors and third party users who have access to confidential information include compliance with information governance requirements, as part of employment or contracting processes.

### Level 3

All pharmacy contracts for staff, contractors and third party users who have access to confidential information include compliance with information governance requirements as part of employment or contracting processes. As the law in this area is subject to change, an annual review is undertaken to assess whether the contractual terms/clauses are still sufficient.

### Hints and Tips

- Ideally, the contract clause should reference the pharmacy's staff confidentiality code of conduct (see information governance requirement 201) as a source of further information about how the pharmacy expects its staff to behave in respect of maintaining the confidentiality and security of patient health information.
- A suggested contract clause for individual staff members can be found online at: [www.psn.org.uk/ig](http://www.psn.org.uk/ig)
- For staff members that don't have a contract of employment, for example locum pharmacists or university students on temporary placement, pharmacies should put in place an agreement which obligates the individuals to safeguard personal information and makes reference to the pharmacy confidentiality code of conduct. The individual could be asked to sign a stand alone confidentiality contract or, where it exists, be asked to sign a written locum contract.
- National Pharmacy Association (NPA) members can obtain guidance on employment matters including employment contracts from the NPA Personnel Department.
- Care needs to be taken to ensure there are also appropriate confidentiality and non-disclosure clauses in contracts with suppliers where they may have access to personal or sensitive information, for example PMR system suppliers.

## Evidence

Level	Evidence Required	Resources Available	Yes/No
1	Example contract clauses	Example contract clause available online at <a href="http://www.psn.org.uk/IG">www.psn.org.uk/IG</a>  Template 2: Stand-alone confidentiality contract	
2	Written confirmation that all staff have appropriate clauses in their contract. (A note here is sufficient)	–	
2	Written confirmation that all temporary staff have appropriate stand alone confidentiality contracts. (A note here is sufficient)	–	
2	List of third party contractors with access to personal information and written confirmation that appropriate confidentiality clauses are included in contracts. (A note here is sufficient)	–	
3	Evidence of annual review of appropriateness of contractual clauses (e.g. date last reviewed)	–	

## Notes

*I confirm that:*

- *all staff have appropriate clauses in their contract .... (date: )*
- *all temporary staff have appropriate confidentiality contracts... (date: )*
- *all third party contractors with access to personal information have appropriate clauses in their contracts ..... (date: )*

*The following third party contractors have access to personal information:.....*

## Are pharmacy staff aware of their information governance responsibilities and are they provided with appropriate training?

Pharmacies should put in place measures to ensure that all staff members are fully informed about information governance procedures and staff should be given clear guidelines about their own responsibilities for ensuring and maintaining confidentiality, data protection and security.

### Level 0

The pharmacy does not have documented evidence that staff are aware of information governance procedures.

### Level 1

The pharmacy has identified key staff members requiring information governance training and ensured that appropriate training has been made available and that the availability and importance of training has been publicised to these members of staff.

### Level 2

The pharmacy has in place a clear and communicated process for making all staff who have access to confidential information aware of available training and has ensured that all staff members who have access to confidential information have been given the opportunity and actively encouraged to undertake information governance training.

Ideally all new staff members who have access to confidential information should be provided with training within a short time of taking on their post.

### Level 3

The pharmacy has a formal targeted information governance training programme which all staff must undertake on a compulsory basis.

## Hints and Tips

- **Paper-based training package:** PSNC and the RPSGB have worked with DH Informatics to publish a training booklet for staff entitled, "Introduction to Information Governance for Pharmacy Staff". This was sent to all pharmacies in January 2010. The training booklet can also be downloaded from the PSNC Website ([www.psn.org.uk/IG](http://www.psn.org.uk/IG)) and additional hardcopies are available on request (while stocks last) by contacting the PSNC Office (01296 432823).



- **The Information Governance Training Tool:** The Information Governance Policy team within DH Informatics in conjunction with the PSNC and RPSGB has developed an e-learning module for pharmacy staff, which is available via the online Information Governance Training Tool. This can be accessed online at [www.connectingforhealth/igtrainingtool](http://www.connectingforhealth/igtrainingtool). The Training Tool includes a module specifically for pharmacy staff titled 'Introduction to Information Governance'. To access the tool, users need to set up an account and as part of the registration process users will be asked for their organisation's ODS Code (for pharmacies, this code begins with the letter F and can be found on the submission document used to send prescriptions to NHS Prescription Services each month). The resource can also be accessed without registering by taking the 'guest tour'. It is not necessary to have an email address to access or register for the tool.
- Other equivalent training resources may also be used to meet this requirement, for example in-house training packages produced by multiple pharmacies or, where available, PCT provided training.

**Evidence**

Level	Evidence Required	Resources Available	Yes/No
1	List of training resources used (e.g. note below)	Online and paper-based training packages	
1	Signature list confirming key staff have received training	Template 14: Staff Signature List	
2	Signature list confirming all relevant staff have received training	Template 14: Staff Signature List	
3	Evidence that training is compulsory, e.g. that it is included in the Staff Induction programme (e.g. note below on pharmacy arrangements)	-	

**Notes**

*The training resources used by staff are .....*

*Training for all new staff is provided by .....*

## Has the pharmacy implemented robust IG arrangements to ensure the NHS CFH IGSoC is satisfied?

The NHS Information Governance Statement of Compliance (IGSoC) is the formal agreement containing the terms and conditions required by NHS CFH of all organisations wishing to directly access N3.

Completion of this requirement is only relevant if a pharmacy has a direct connection to N3. This majority of pharmacy sites connect indirectly via a commercial 'aggregator' or corporate connection and are therefore not required to complete the IGSoC Agreement.

The IGSoC terms and conditions incorporate IT technical requirements and a requirement to achieve, or have an agreed action plan in place to achieve, the NHS information governance requirements published through the IG Toolkit. By accepting the IGSoC terms and conditions, an organisation also agrees to IGSoC compliance monitoring by NHS CFH which may take the form of on-site audits, and to submit annual IG assessments using the Information Governance Toolkit.

### Not Applicable

The IGSoC is only relevant to those organisations that have direct connections to the N3 network. Therefore, if a pharmacy site has N3 access via a 'network aggregator' such as InTechnology plc, IMS or Vialtus it will not need to complete the IGSoC process. Likewise where a pharmacy connects to N3 via a corporate network, the Head Office must complete the IGSoC but not each individual site.

Where there is an indirect connection to N3, the pharmacy must provide assurance to the PCT that their aggregator or Head Office has completed the IGSoC process. To do this, the requirement should be marked as not applicable and the following comments should be entered into the comments box in the online IG Toolkit:

- Confirmation that the pharmacy has an indirect connection to N3;
- the name of the network aggregator (e.g. 'IMS');
- the location of evidence (e.g. confirmation letter) of assurances obtained from the aggregator regarding completion of the IGSoC process.

If a pharmacy is not yet connected to N3 either directly or indirectly, for example the pharmacy has not yet deployed the Electronic Prescription Service, the requirement should also be marked as 'not relevant' when the online IG Toolkit is completed. In the comments box, state that the pharmacy does not yet connect to N3.

### Level 0

The pharmacy is required to complete IGSoC but does not satisfy the requirements for NHS CFH IGSoC compliance and has not agreed plans for achieving compliance within timescales acceptable to the PCT.

### Level 1

IGSoC compliance requires the pharmacy to work with requirements across the IG Toolkit. The pharmacy should review as a priority improvement plans for the following key requirements: 114, 116, 117, 119, 201, 208, 209, 212, 305, 308, 317, 320. Where the pharmacy has not reached level 2, plans to reach the required standard must be agreed with the local PCT.

### Level 2

The pharmacy complies, at attainment level 2 with all of its current NHS CFH IGSoC.

### Level 3

The pharmacy continues to comply with all requirements of its current NHS CFH IGSoC. It has also implemented an independent audit and assurance programme that ensures the completeness and accuracy of its assessed IGSoC compliance.

### Hints and Tips

- If you have any questions about whether your pharmacy connects to N3 and whether this is directly or indirectly, contact your pharmacy system supplier for more information.
- More guidance on IGSoC is available online at: [www.connectingforhealth.nhs.uk/igsoc](http://www.connectingforhealth.nhs.uk/igsoc). Support is available from the NHS CFH Exeter Helpdesk ([exeter.helpdesk@nhs.net](mailto:exeter.helpdesk@nhs.net)) Phone: 01392 251289.

**Evidence**

Level	Evidence Required	Resources Available	Yes/No
NA	Note below confirmation that the pharmacy accesses N3 via an indirect connection (Majority of pharmacies)	-	
1	Documentary evidence of review against improvement plan for prioritised requirements	-	
2	Evidence that Level 2 compliance reached for each of the pharmacy requirements.	-	
3	Evidence of continued compliance	-	
3	Evidence of Independent audit and assurance.	-	

**Notes**

*I confirm that the pharmacy has an indirect connection to N3:  
yes/no*

*If yes, the name of the network aggregator (e.g. IMS, Vialtus etc.)  
or indicate if your Head Office has arranged a corporate connection:*

*Evidence (e.g. confirmation letter) of assurances obtained from your  
connectivity provider or Head Office regarding completion of the  
IGSoC process is stored .....*

## Does the pharmacy ensure that staff and all those working for or on behalf of the pharmacy comply with the terms and conditions set out in the RA01 form?

The NHS CFH Registration Authority form (RA01) sets out a number of specific conditions governing the use of the smartcards and the NHS Care Records Service (CRS) applications to which these permit access. These conditions include specific requirements around the safe and secure retention of smartcards and the notification of any changes to the user's access profiles.

In Release 2 of the Electronic Prescription Service (EPS), dispensing contractors will have access to a part of the NHS CRS known as the Personal Demographics Service. Therefore, dispensing contractors and their staff will be required to adopt the 'single smartcard' access model and sign up to the conditions set out in the RA01 form. Pharmacy contractors were not required to sign up to these terms for access to EPS Release 1.

Pharmacy contractors are required to ensure staff comply with the RA01 requirements and understand that failure to do so will be dealt with as a serious disciplinary matter.

### Not Applicable (NA)

If staff do not have cards subject to the RA01 terms and conditions, this requirement is not applicable. However note that pharmacy staff will be required to sign up to these terms to obtain access rights to EPS Release 2 functionality. If declaring that this requirement is not applicable, make a note in the comments box on the online Information Governance Toolkit that staff do not yet have cards subject to the RA01 terms and conditions.

### Level 0

The pharmacy does not have documented evidence that the terms and conditions set out on the RA01 form are monitored and enforced.

### Level 1

The pharmacy does not monitor to ensure that staff comply fully with the terms and conditions set out within the RA01 form but has developed a process for doing so. The process must be agreed by an appropriate senior staff member.

### Level 2

The pharmacy has implemented its process for monitoring and enforcing compliance with the terms and conditions set out in the RA01 form.

### Level 3

The pharmacy ensures that all staff are aware of their responsibilities and that the terms and conditions set out in the RA01 are fully enforced. The pharmacy's approach to sustaining this is reviewed annually, staff performance is monitored and remedial action taken swiftly when required.

### Hints and Tips

- Detailed guidance on the arrangements for obtaining smartcards can be found on the PSNC website ([www.psn.org.uk/smartcards](http://www.psn.org.uk/smartcards)).
- Audit checks on whether the procedures are being followed could be carried out by the information governance Lead or a senior staff member, for example the pharmacist.

**Evidence**

Level	Evidence Required	Resources Available	Yes/No
NA	If no staff have cards subject to the RA01 terms and conditions, this requirement is not applicable.	–	
1	Description of process to undertake compliance checks (make a note below)	–	
2	Evidence of internal audits to assess compliance with the RA01 terms (e.g. every 6 months)	Template 13: Audit sheet (e.g. provide dated last audit outcome)	
2	Evidence staff have read the RA01 Terms and Conditions	Template 14: Staff signature List	
3	Evidence that the audit process is reviewed annually (e.g. date process last reviewed)	–	

**Notes**

*Who undertakes the audit checks?.....*

*How often are audits undertaken?.....*

*What checks are undertaken? (e.g. cross-reference an audit checklist).....*

## Does the pharmacy have a confidentiality code of conduct that provides staff with clear guidance on the disclosure of personal information?

To ensure staff members are effectively informed of their obligations to keep information confidential, pharmacies should develop a staff code of conduct that provides clear guidance on the disclosure of personal information. The code should be signed off by a senior staff member authorised by the contractor and should be made available to staff.

### Level 0

The pharmacy does not have a confidentiality code of conduct for staff.

### Level 1

The pharmacy has a confidentiality code of conduct for staff that provides clear guidance on the disclosure of personal information and which has been signed off by an appropriate senior manager.

### Level 2

The pharmacy's approved confidentiality code of conduct has been made available to all staff members who have been effectively informed about the code and the guidance on disclosure and the need to comply with it.

### Level 3

Compliance with the code is monitored.

## Hints and Tips

- Where a pharmacy already has a general code of conduct, it may be possible to extend this rather than having a separate confidentiality code.
- Key components of a confidentiality code of conduct are:
  - The legal framework governing confidentiality;
  - Staff members' individual responsibility for compliance with the law;
  - Definition of information that is considered confidential;
  - How to ensure information remains confidential;
  - Guidelines on passwords, smartcards and security;
  - The systems and processes for protecting personal information (safe havens, devices and systems for secure storage etc.);
  - Use of email and web-based services;
  - The circumstances under which confidential information can be disclosed;
  - Dealing with subject access issues;
  - Abuse of privilege in respect of viewing personal information;
  - Offsite/home working arrangements (where relevant);
  - Who to approach for assistance with disclosure issues (e.g. information governance Lead); and
  - Possible sanctions for breach of confidentiality.
- Requirement 212 requires documented guidelines on seeking patient consent for purposes other than the service for which it was collected, including the sharing of information. These guidelines could also be included in the confidentiality code of conduct.

## Evidence

Level	Evidence Required	Resources Available	Yes/No
1	Staff confidentiality code of conduct	Template 3: Confidentiality Code of Conduct	
1	Name of contractor representative that approved the confidentiality code of conduct (e.g. make note below)	-	
2	Evidence that staff have been made aware of the confidentiality code of conduct e.g. staff signature list	Template 14: Staff signature list	
2	Evidence that the confidentiality code of conduct is available in the pharmacy (e.g. note below where it is stored)	-	
3	Internal audit of staff understanding of the confidentiality code of conduct and their obligations (e.g. every 6 months)	Template 13: Audit sheet (e.g. provide dated last audit outcome)	
3	Evidence (e.g. date) of last review of the confidentiality code of conduct	-	

## Notes

*The name of the senior staff member that approved the confidentiality code of conduct is .....*

*The confidentiality code of conduct is stored in the pharmacy in .....*

*The confidentiality code of conduct was last reviewed .....*

## Has the pharmacy mapped all flows of personal information, assessed risks in line with Department of Health guidelines and put in place safe haven procedures for all routine flows of personal information to the organisation?

A key requirement of information governance assurance is to map and record all routine flows of personal information into and out of the pharmacy. This is then used to identify risks associated with data transfer so that appropriate measures can be taken to remove or mitigate the risks.

### Level 0

The pharmacy has not mapped any flows of personal information and does not have documented evidence that it operates safe haven procedures for personal information that flows routinely into the organisation.

### Level 1

The pharmacy has identified its routine flows of personal information and assessed risks in flow methods with remedial action immediately taken where significant risks were highlighted.

A documented safe haven procedure has been developed for the receipt of routine flows of personal information.

### Level 2

The information governance Lead is aware of all risk areas identified in the mapping exercise.

The safe haven procedures have been signed off by a senior manager and implemented. All staff members who receive personal information (including temporary staff) have access to the procedures and have been made aware of the location of safe havens.

### Level 3

The pharmacy undertakes an annual review of its mapped flows of personal information and ensures that records are updated to reflect any changes in flow methods, locations or data items.

The pharmacy monitors the use of safe havens for its inbound flows of personal information and has put in place processes to ensure compliance and appropriate use.

### Hints and Tips

- Guidance on mapping and risk assessing information flows can be found in Appendix 7.
- Risks should be recorded. This record is sometimes referred to as a 'risk register'. The template information flow map and table in appendix 7 could serve as your risk register.
- Safe havens are all secure points at which confidential information is received.

## Evidence

Level	Evidence Required	Resources Available	Yes/No
1	Evidence of mapping information flows and the recording of risks	Template map of information flows (Appendix 7) (which can form the risk register)	
1	Safe haven procedures	Template 4: Data handling SOP	
2	Name of contractor representative that approved safe haven procedures (e.g. note below)	–	
2	Evidence that staff have been made aware of the safe haven procedures	Template 14: Staff signature list	
2	Evidence that staff have access to the safe haven procedures (e.g. note the location they are stored below)	–	
3	Evidence of internal audit checks on compliance with safe haven procedures (e.g. every six months)	Template 13: Audit sheet (e.g. provide dated last audit outcome)	

## Notes

*The contractor representative that approved procedure: .....*

*The procedures are stored in the pharmacy in .....*

## Does the pharmacy ensure that all personal data processed outside of the UK complies with the Data Protection Act 1998 and DH guidelines?

DH guidelines are more restrictive than the Data Protection Act and these require that personal information is **NOT** transferred outside of the UK unless an appropriate assessment of risk has been undertaken and mitigating controls put in place. Pharmacies are required to ensure that all personal data processed outside the UK complies with the Data Protection Act 1998 and DH guidelines.

### Level 0

The pharmacy does not know whether or not personal data is transferred from the pharmacy to countries outside of the UK.

### Level 1

The pharmacy has carried out an assessment and documented instances where personal data is transferred to non-UK countries and whether any such transfer complies with the Data Protection Act 1998 and DH guidelines. Where necessary, the pharmacy has taken measures to enable full compliance with the legal requirements and DH guidelines.

### Level 2

The pharmacy has assessed all transfers of personal data from the pharmacy to countries outside of the UK and ensures any transfers fully comply with the Data Protection Act 1998 and DH guidelines.

### Level 3

The pharmacy annually reviews its transfers of personal data to non-UK countries and ensures continuing compliance with the Data Protection Act 1998 and DH guidelines.

## Hints and Tips

### Steps for a pharmacy to ensure compliance

#### Step 1:

Review the flows of personal information to external organisations (recorded for requirement 208) to understand whether any such information flows outside of the UK, for example:

- If personal information is collected through a pharmacy website, where is the website hosted?
- If an IT system is used to record information, for example the PMR system or systems to support the delivery of enhanced services, where is this information hosted and does the supplier ensure the information remains within the UK?

Where the pharmacy has determined that it makes no transfers of personal information to countries outside of the UK this should be documented for audit purposes (e.g make a note in the notes box).

#### Step 2:

If the review has identified flows of personal information to countries outside of the UK, undertake an appropriate risk assessment and put in place mitigating controls.

In assessing risk, a key consideration is whether the off-shore providers' security arrangements have been independently verified. For example, if the relationship is between the contractor and an international provider, has the provider achieved the recognised ISO 27001 Information Security Management standard (which includes a requirement to have independent verification)? If the relationship is with a UK provider who sub-contracts to an overseas provider,

have they achieved the CFH IGSoC standards or ISO 27001? Controls could include seeking assurances from system suppliers (and, where applicable, their subcontractors) through contractual arrangements about the processes and safeguards in place for offshore data transfer.

Decisions concerning the transfer of personal information to countries outside of the UK must only be taken by a senior pharmacist/manager who has been authorised to take that decision by the contractor.

**Step 3:**

Consider the other data protection principles before making an overseas transfer of personal data, in particular, the first principle, which in most cases will require that individuals are informed about the transfer of their information to a country outside the UK.

**Future proofing the arrangements:**

A supplier may change their arrangements over time. When contracts with suppliers are being

reviewed, it is worth considering whether to include clauses that would ensure a contracted system supplier would proactively inform the pharmacy if their offshore data transfer arrangements change.

More information on the relevant guidance in the Data Protection Act and DH guidance can be found in Appendix 4.

**Evidence**

Level	Evidence Required	Resources Available	Yes/No
1	Evidence the pharmacy has checked whether there are flows of information outside of the UK and documented these flows (e.g. note below)	–	
2	If there are flows of information outside of the UK, evidence of assessment of compliance with the Data Protection Act and DH guidance (e.g. note below)	–	
3	If there are flows of information outside of the UK, details of any action plan followed to secure compliance with the Data Protection Act 1998 and DH guidelines (e.g. note below)	–	

**Notes**

**Does the pharmacy ensure that patients are generally asked before their personal information is used for purposes that are not directly related to the service for which it was collected, and that patients' decisions to restrict the disclosure of their personal information are appropriately respected?**

Pharmacies are required to have procedures for seeking consent. These should include seeking consent to use patient information for purposes other than the service for which it was collected, and on respecting patient decisions.

### Level 0

The pharmacy does not have documented evidence that they ensure that patients are asked before their personal information is used for purposes that are not directly related to the service for which it was collected and ensure that patient's decisions to restrict the disclosure of their personal information are appropriately respected.

### Level 1

The pharmacy has guidelines on seeking consent to use personal information including for purposes that are not directly related to the service for which the information was collected, and on respecting patient decisions. These guidelines have been approved by a senior contractor representative. The guidelines could be added to the staff confidentiality code of conduct (Requirement 201).

### Level 2

The pharmacy has ensured that all relevant staff members have been effectively informed about the guidelines and the need to comply with them.

### Level 3

The pharmacy monitors staff compliance with the guidelines through regular checks e.g. random checks with staff and patients, patient awareness/satisfaction surveys.

### Hints and Tips

- Areas that the guidelines and procedures could cover:
  - When and how consent should be obtained;
  - How patients are made aware of who may have access to personal information held about them, and the extent to which the information may need to be shared;
  - The basic premise that patients have the right to choose (i.e. consent given or not) whether or not to agree to the use or disclosure of their personal information. Note, in some cases this may impact on whether the service can be provided;
  - The right of patients to change their decision about a disclosure before it is made;
  - Who should obtain consent for the use of the information for a further purpose (NB while the task can be delegated, the pharmacy owner remains legally responsible);
  - Where and how consent or dissent should be recorded;
  - Answering patient questions about consent, including how to provide information about the consequences of non-disclosure to patients in a non-threatening, non-confrontational manner;
  - How often consent should be reviewed; and
  - Exemptions to the requirement for consent – public interest; legally required; and section 251 of the NHS Act 2006 (formerly section 60 of the Health & Social Care Act 2001).
- More detailed information on confidentiality, consent and the law can be found in Appendices 4 and 5.

**Evidence**

Level	Evidence Required	Resources Available	Yes/No
1	Evidence of guidelines on seeking patient consent to use their information (this could form part of the confidentiality code of conduct)	Template 3: Staff confidentiality code of conduct	
1	Name of contractor representative that approved guidelines on seeking patient consent to use their information (note below)	-	
2	Evidence that staff have been made aware of the guidelines e.g. staff signature list	Template 14: Staff signature list	
3	Internal audit of staff compliance with the guidelines (e.g. every 6 months)	Template 13; Audit sheet (e.g. provide dated last audit outcome)	

**Notes**

*The name of the senior staff member that approved the guidelines on seeking patient consent to use their information is .....*

## Does the pharmacy have a publicly available and easy to understand patient information leaflet that informs patients how their information is used, who may have access to that information, and their own rights to see and obtain copies of their records?

To support patient awareness each pharmacy should have an information leaflet for patients about the way that their information is used and shared. This leaflet should be placed in a part of the pharmacy where patients are likely to see and read the leaflet (for example, on the front counter or in the consulting area).

### Level 0

The pharmacy does not make any information about the use of personal information available to patients.

### Level 1

Basic information about the use of personal data is made available to patients.

### Level 2

In addition to basic information the pharmacy makes more comprehensive information available via a leaflet.

### Level 3

The pharmacy ensures that pharmacy staff are able to support patient understanding of how their information is used, who may have access to that information, and patients' rights to see and obtain copies of their records.

## Hints and Tips

### Level 1

- The community pharmacy contractual framework requires pharmacies to have a 'practice leaflet' which includes a notice that the pharmacy complies with the Data Protection Act and the NHS Code of Practice on Confidentiality. This is sufficient to meet the Level 1 requirement.

### Level 2

- To meet the Level 2 requirement, pharmacies must make more comprehensive information available. The information leaflet should cover:
  - How patient information is used and stored;
  - Who is able to access patient information;
  - How patients can gain access to their information; and
  - Who they can talk to for more information (e.g. the pharmacist).
- Rather than having a separate information governance leaflet, some pharmacies may want to adapt and expand the content in existing practice leaflets.
- A professionally printed leaflet may be available to purchase from organisations such as the NPA. Some PCTs may have printed generic leaflets for use by health professionals in their area.

### Level 3

- Key points to consider including in a briefing for a staff are how they can:
  - incorporate checks within their everyday working practice that patients have seen available

- information leaflets;
  - make clear to patients when information is recorded and accessed;
  - make clear to patients when information is, or may be, disclosed to others;
  - check that patients are aware of
    - The community pharmacy
- the choices available regarding disclosure;
  - deal with concerns or queries; and
  - respect the right of patients to have access to their health records.
- contractual framework requires pharmacies to conduct an annual patient survey. A question could be added to the survey to assess patient awareness of the patient leaflet, to meet the Level 3 requirement.

## Evidence

Level	Evidence Required	Resources Available	Yes/No
1	Basic information for patients on confidentiality, through a leaflet or poster	A pharmacy's existing practice leaflet should meet this requirement	
2	Comprehensive patient information e.g. leaflet	Template 5: Confidentiality leaflet	
3	Evidence that staff have been briefed on how the pharmacy uses patient information and how to discuss this with patients	Template 14: Staff signature list	
3	Evidence of patient awareness of the patient leaflet and how they can obtain more information about how their personal information is used (note below e.g. question in the annual patient survey)	–	

## Notes

## Does the pharmacy ensure that there are appropriate procedures in place to manage access to computer-based information systems?

The pharmacy should put in place procedures to manage staff access to computer-based information systems (e.g. PMR) that store personal information. This includes the allocation and removal of user accounts and guidelines for pharmacy staff to ensure they use information systems appropriately. The procedures should be regularly reviewed and audits undertaken to ensure compliance.

### Level 0

The pharmacy does not have documented evidence that there are appropriate procedures in place to manage access to computer-based information systems.

### Level 1

The pharmacy has documented procedures for allocating and managing access controls for users of pharmacy information systems.

### Level 2

The pharmacy has implemented its procedures and ensures that access to the pharmacy system is restricted to authorised users only.

### Level 3

The pharmacy has in place a process to monitor compliance with its access management procedures.

## Hints and Tips

### Extent of Access Controls

- Ideally, all pharmacy users should be assigned an individual user ID. However, there is a balance between security and usability of systems, and it is recognised that individual staff logins may not be a practical option at this time, for example to control access to the PMR system by pharmacy staff. Decisions on the extent of access controls applied should be taken by the pharmacy contractor based on the risks of unauthorised access, the nature of the data and the impact on pharmacy workload of any controls.
- The access control functionality in PMR systems is likely to develop over time. This is linked to work being carried out by NHS CFH.

### Developing Access Management Procedures

Key points that the procedure should cover are:

- Scope of the procedures
- A summary of the technical access controls in place  
*Contact your system supplier as necessary for more information.*
- Procedure for granting access and which level of access  
*For example, who is responsible within the pharmacy for making decisions on access rights? What arrangement is in place for locums who need temporary access?*
- Procedure for managing changes in access rights  
*For example, if a user leaves the organisation, their profile would need to be suspended or removed.*
- Procedures for staff in relation to logging in to the system  
*Pharmacy systems may provide password protection features such as:*
  - Users must change their password after the first logon;
  - Users must specify complex passwords;
  - Users must change their passwords periodically;
  - Prevention of password reuse;
  - User may change their password at their request.
- Requirements for periodic review of the procedures  
*The procedures will need to take account of changes made to the technical access controls in systems by pharmacy system suppliers.*

**Evidence**

Level	Evidence Required	Resources Available	Yes/No
1	Evidence of access control procedures	Template 15: Access control procedures	
2	Name of contractor representative that approved the access control procedures (e.g. note below)	-	
3	Internal audit of staff compliance with access control procedures (e.g. every 6 months)	Template 13: Audit sheet (e.g. provide dated last audit outcome)	

**Notes**

*The name of the senior staff member that approved the access control procedures is .....*

## Does the pharmacy ensure that digital information shared with other organisations is secured in transit?

Pharmacies must have procedures in place to ensure security and confidentiality of patient information is maintained when using digital transfer methods such as email.

### Level 0

The pharmacy does not have documented evidence that they ensure that digital information exchanged with other organisations is done so securely.

### Level 1

The pharmacy has identified with whom, where and how digital information is exchanged.

### Level 2

The pharmacy has data handling procedures in place to ensure digital information is adequately protected in transit and only exchanged in accordance with NHS Codes of Practice and NHS information governance standards. Relevant staff members are effectively informed about the secure transit requirements of digital information, in particular by email.

### Level 3

The pharmacy regularly reviews its data handling procedures and carries out monitoring to ensure that digital information is handled in accordance with the procedures.

### Hints and Tips

- Possible modes of digital exchange of information are: eFax, email, instant messaging (IM), portable data storage devices, secure messaging, SMS Messaging, web interfaces.
- Information that is transferred through the NHS CRS (including EPS) does not need to be considered as it is protected by the robust access control and confidentiality framework developed by NHS CFH.
- Detailed guidance on the risks involved in using different data transfer methods can be found in Appendix 6. Pharmacies should take particular care with using portable data storage devices such as data sticks and email communications.
- The technical aspects of the security and encryption of electronic communications will be beyond the control of pharmacies. Requirement 116 covers contractual controls for third parties.

## Evidence

Level	Evidence Required	Resources Available	Yes/No
1	Evidence the pharmacy has mapped with whom, where and how digital information is exchanged (links to Requirement 208)	Data mapping template (Appendix 7)	
2	Evidence of data transfer procedures (links to Requirement 208)	Template 4: Data transfer SOP	
2	Name of contractor representative that approved the data transfer procedures (e.g. note below) (links to Requirement 208)	–	
2	Evidence that staff have been made aware of the data transfer procedure e.g. staff signature list (links to Requirement 208)	Template 14: Staff Signature List	
3	Internal audit of staff compliance with the data transfer procedure e.g. every 6 months (links to Requirement 208)	Template 13: Audit sheet (e.g. provide dated last audit outcome)	
3	Evidence of regular (e.g. annual) review of the data transfer procedure (e.g. date last reviewed) (links to Requirement 208)	–	

## Notes

*The name of the senior staff member that approved the data transfer procedure is .....*

*The data transfer procedure was last reviewed .....*

## Does the pharmacy have an information asset register, encompassing information, software and hardware?

Unless pharmacies know the type of information assets they possess it will be very difficult to ensure that each item is adequately protected through appropriate confidentiality and security measures. Pharmacies are required to maintain a record of information assets in the form of a register.

### Level 0

The pharmacy does not have an asset register encompassing information, software and hardware.

### Level 1

The pharmacy has assigned responsibility to a staff member to compile information about the pharmacy's assets and to maintain an asset register.

### Level 2

The pharmacy has an information asset register encompassing information, software and hardware.

### Level 3

The pharmacy has an information asset register which is maintained, regularly reviewed and updated as necessary.

## Hints and Tips

### Content of an Information Asset Register:

Categories of information asset that should be considered are:

- **Information:** e.g. patient databases, archived information;
- **Software:** e.g. applications, development tools and utilities;
- **Physical:** e.g. IT equipment, removable media.

There are no mandatory requirements for how the register should be structured however pharmacies should ensure useful information is captured to enable them to comply with the objective of this requirement. For example the entry for a physical asset such as a computer may include:

- Its physical location;
- What NHS and/or personal information is included on it;
- Details of those responsible for the maintenance of the computer; and
- Who to contact if something goes wrong.

**Maintaining the register:** Different pharmacies are likely to maintain the register in different ways. In the case of multiples, this information may be stored at Head Office. In this case, evidence of the existence of the register may be a declaration from Head Office.

**Information asset owners:** It is important that the asset is linked to a post, rather than a person, as responsibilities linked to people tend not to get passed on when that person changes job.

**Sharing Information with PCTs:** As information asset registers are likely to include commercially sensitive information, there is no requirement for the details of the register to be shared with PCTs. Acceptable evidence that the register exists and it is up to date is the date that the register was last updated and where it is stored.

**Evidence**

Level	Evidence Required	Resources Available	Yes/No
1	Evidence of assignment of responsibility for maintaining the asset register (e.g. note below)	–	
2	Location of information asset register (e.g. note below)	Template 6: Data asset register	
3	Evidence of review of information asset register (e.g. note date last reviewed below or note if policy is to review when new asset obtained or old asset de-commissioned)	–	

**Notes**

*The staff member responsible for maintaining the information asset register is .....*

*The information asset register is located .....*

*Date of last review .....*

## Does the pharmacy prevent unauthorised access to the pharmacy premises, equipment, records and other assets?

Pharmacies are required to undertake a risk assessment to identify areas at risk of unauthorised access to hardware, software and information. Where necessary, the pharmacy should take steps to implement the necessary improvements. Staff should be aware of the measures to take in the event of unauthorised access.

### Level 0

The pharmacy does not have documented evidence that they have taken measures to prevent unauthorised access to pharmacy premises, equipment, records and other assets.

### Level 1

The pharmacy has undertaken a risk assessment and has identified areas of concern but has not carried out the improvements necessary to prevent unauthorised access to the premises equipment, records and other assets.

The pharmacy has put in place measures to ensure that all staff are aware of what steps to take in the event of unauthorised access.

### Level 2

The pharmacy has begun to implement any improvements necessary to prevent unauthorised access to the premises, equipment, records and other assets e.g. by developing an action plan, allocating necessary resources, etc.

### Level 3

The pharmacy has taken all reasonable measures to prevent unauthorised access to the premises, equipment, records and other assets by making any necessary improvements.

## Hints and Tips

- Pharmacies have well established procedures for premises security as a matter of course and large pharmacy organisations often have sophisticated commercial asset and risk management procedures in place. If no security improvements are required following the risk assessment, simply note this.
- A template risk assessment is available. If pharmacies develop their own, areas to consider are:
  - The Dispensary (ensuring it is not left unoccupied)
  - Consultation area (ensuring paperwork such as prescriptions or MUR forms containing personal information are not left unattended)
  - Window security
  - Back doors and fire escapes
  - Burglar alarms
  - Keys and staff Access
  - Clear desk and clear screen policy (e.g. use of screensavers)
- If necessary, specialist guidance on security may be available from loss adjustment/commercial risk advisers.

**Evidence**

Level	Evidence Required	Resources Available	Yes/No
1	Documented risk assessment	Template 7: Risk assessment template	
1	Evidence of staff guidance on steps to take in the event of unauthorised access (e.g. note guidance below)	-	
2	Evidence of work to implement high priority security improvements identified by risk assessment (e.g. detail below or note if none were required)	-	
3	Evidence of work to fully implement security improvements identified by risk assessment where required (e.g. detail below or note if none were required)	-	

**Notes**

*The risk assessment is located.....*

*In the event of unauthorised access to information, staff should .....*

*Were security improvements identified by risk assessment? Yes/no*

*If yes, what work was undertaken to implement high priority security improvements identified by the isk assessment .....*

*If yes, what work was undertaken to fully implement security improvements identified by the risk assessment .....*

## Does the pharmacy control, monitor and audit the use of mobile computing systems to ensure their correct operation and to prevent unauthorised access?

Pharmacies are required to record staff use of mobile devices, provide staff with good practice guidance on the secure use of devices and ensure that the guidelines are being followed in practice.

### Not Applicable (N/A)

This requirement only applies to pharmacies using mobile computing systems (e.g. laptops and PDAs). If declaring that this requirement is not applicable, make a note in the comments box on the online Information Governance Toolkit that the pharmacy does not use any mobile computing systems.

### Level 0

The pharmacy does not have documented evidence that they control, monitor and audit the use of mobile computing systems to ensure their correct operation and to prevent unauthorised access.

### Level 1

The pharmacy keeps a record of staff use of mobile computing equipment and staff have been issued with basic guidelines on the confidentiality and security risks of using mobile computing equipment.

### Level 2

The pharmacy has implemented procedures on security and confidentiality including more comprehensive guidance for staff, so that the use of mobile computing systems for pharmacy work is controlled.

Maintenance of patient confidentiality could be better achieved through encryption of all mobile computing systems to NHS standards, although staff must still be provided with advice to ensure equipment is not stolen or lost.

### Level 3

The pharmacy ensures that the use of mobile computing systems is controlled, monitored and audited to ensure:

- Correct operation and prevent unauthorised access to those systems;
- All users comply with procedures and guidance;
- All mobile device and removable media assets can be accounted for;
- Secure remote access to the pharmacy system is possible and is used (where relevant); and
- Sensitive or confidential information is encrypted, securely transported or stored in secure locations.

### Hints and Tips

*The actions taken to protect mobile computing systems should be proportionate to the risks in the environment.*

**Guidance to staff:** Areas that could be covered in guidance to staff are:

- Locking the machine up overnight, or removal of the hard-drive or memory card (where possible) if the machine cannot be locked away;
- Not leaving the device unattended, e.g. on the seat of a car;
- Use of secure passwords to prevent unauthorised access to information stored on the computer;
- Ensuring password security; and
- Reporting the loss or theft of equipment promptly.

**Encryption:** Personal data stored on a PC hard-drive or other removable device in a non-secure area or on a mobile computing device such as a laptop, PDA or mobile phone should be encrypted. It is recognised however that this may take some time to achieve. As an interim measure, if following a risk assessment it is felt that continued reliance upon unencrypted data is necessary for the benefit of patients, the outcome of the risk assessment must be reported to the most senior person in the pharmacy, so that he/she is appropriately accountable for the decision to accept data vulnerability or to curtail working practices in the interests of data security. Guidance on the NHS recommended encryption algorithms can be found in Appendix 6.

For pharmacies that have obtained hardware from their pharmacy system supplier, expert advice on encryption should be sought from the supplier.

## Backing-up and Maintaining Anti-virus Protection

Mobile devices such as laptops are best configured so that data processed on them is synchronised to the network at the end of a session. If data is only saved to a local drive and the device is lost or damaged, so is the data. Only the minimum amount of data required should be carried on mobile devices to reduce the potential impacts of an unforeseen event.

Care must also be taken to ensure that all mobile devices have their anti-

virus / anti-spyware components regularly updated to protect against these types of attacks.

## Other Safeguards

Consideration should also be given to strong access controls, user identification and authentication, secured wireless networks where used and encrypted transfer of information over the internet. These issues are covered in more detail in the sections on transfer of information (308) and access controls (305).

If the staff member is also able to remotely access the pharmacy system, e.g. by dialling in from home, a patient's home or another pharmacy location, this must only be allowed if there is a process of strong authentication through token or biometric mechanisms, e.g. NHS Smartcard. If using a remote access solution, pharmacy contractors should satisfy themselves that applications comply with the NHS Code of Practice on Confidentiality, and seek expert advice where necessary.

## Evidence

Level	Evidence Required	Resources Available	Yes/No
NA	If the pharmacy does not use any mobile computing devices, this requirement is not applicable	–	
1	Record of staff use of mobile computing devices	Templates 9 & 10: Record sheets	
1	Evidence of guidance provided to staff who use mobile computing devices	Template 8: Mobile computing guidelines	
2	Evidence that staff are aware of the guidelines around the use of mobile computing devices	Template 14: Staff signature list	
3	Evidence of internal audits to assess compliance with the guidelines around the use of mobile computing devices (e.g. every 6 months)	Template 13: Audit sheet (e.g. provide dated last audit outcome)	

## Notes

## **Does the pharmacy have documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions?**

This requirement relates to ensuring confidentiality and continuity of access to critical patient information, for example the Pharmacy PMR system, in the event of disruptions such as power and system failures. The detail of this requirement is still being finalised but is expected to involve:

---

### **Level 1**

Putting in place a business continuity plan for critical information systems based on an assessment of risk.

---

### **Level 2**

Testing plans through table-top exercises and walk-throughs.

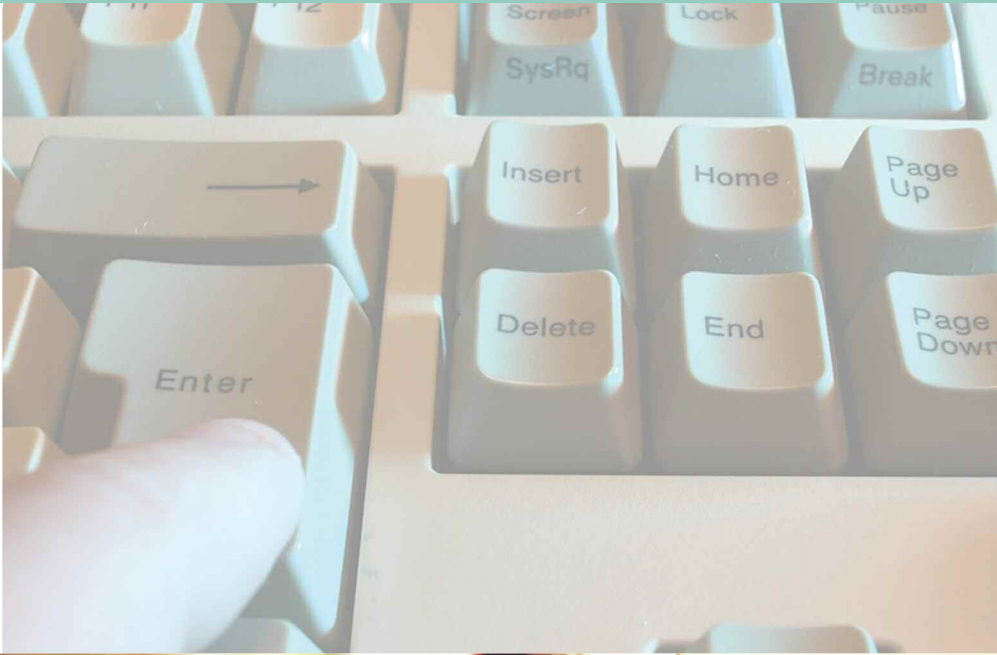
---

### **Level 3**

It is likely that pharmacies will also have to put in place measures to mitigate the risks of interruptions to critical patient information systems and fully test continuity plans by arranging full simulations which may involve joint working with other health professionals, for example GPs.

### ***Hints and Tips***

The details of this requirement and supporting guidance will be finalised in early-mid 2010. This will be communicated to pharmacies via PSNC Community Pharmacy News and will be published on the online Information Governance Toolkit. Pharmacies will need to achieve Level 2 compliance by 31st March 2011.



## Does the pharmacy have documented incident management and reporting procedures?

Pharmacies are required to allocate responsibility for information security to a staff member who can lead on information management and reporting. The pharmacy also needs to have processes in place for managing and documenting information security incidents and staff should be aware of the actions they need to take in the event of an incident.

### Level 0

The pharmacy does not have documented incident management and reporting procedures.

### Level 1

The pharmacy has allocated responsibility for information security to a member of staff who will take the lead on incident management and reporting.

### Level 2

The pharmacy organisation has documented incident management and reporting procedures. All pharmacy staff are effectively informed about the incident management and reporting procedures so that they are aware of action to take in the event of an incident.

### Level 3

The incident management and reporting procedures are reviewed following an incident.

## Hints and Tips

**Incident Management Procedures:** These procedures should detail:

- The need for and scope of the procedure;
- Procedures to be followed when incidents occur (managing incident, recording and reporting incident);
- Responsibilities of staff; and
- Any linked procedures referenced (e.g. the pharmacy data handling SOP).

**Information Security Incident Log:** All information security incidents should be documented, for example in an incident reporting log. The information that should be recorded should include:

- Date of incident (if identifiable);
- Location of incident (if identifiable);
- Details of staff involved (if identifiable and applicable);
- Description of incident;
- Degree of risk associated with the incident (correlates with risk assessment for data transfer);
- Any contributing factors;
- Remedial action taken following this incident;
- Suggested action to be taken to prevent a reoccurrence of this incident; and
- Whether the insurer has been informed.

Incidents should be classified in the log according to severity of risk. Risk assessment methods commonly categorise incidents according to the likely consequences (for example, on a scale of insignificant to critical). Risk assessment guidance can be found in Appendix 7.

**Analysing and learning from incidents:** Pharmacies have for some time been required to record and analyse safety incidents in relation to medicines. The underlying principles are equally applicable to the management of information security incidents. These include:

- Establishing that an incident has, in fact, occurred;
- Establishing that the responsibility for the incident lies with the pharmacy;
- Evaluating the extent of the damage or risk to the pharmacy as a result of the incident;
- Taking timely and appropriate remedial action; and
- Reviewing procedures to reduce the risk of the incident occurring again.

**Reporting information security incidents:** The procedures for reporting information security incidents should be documented in the pharmacy's incident management SOP. The information governance Lead and Information Security Lead (if different) should normally be routinely informed of incidents that occur. It may be appropriate to report the incident to others including the pharmacy insurer and senior management. Although it is not mandatory to inform PCTs of information security

incidents, the pharmacy information governance Lead or information security lead may wish to consider whether it is appropriate to inform the PCT of serious incidents, for example if this is likely to lead to a patient complaint. Consideration should also be given to making a report to the police, for example in the event of data theft. It is also considered best practice to inform the Information Commissioner if the data loss is serious.

## Evidence

Level	Evidence Required	Resources Available	Yes/No
1	Written assignment of responsibility for information security to staff member or members	–	
2	Documented incident management procedures	Template 11: Information security incident management SOP	
2	Documented incident management reports	Template 12: Information security incident log	
2	Evidence staff have been informed of information security incident management procedures	Template 14: Staff signature sheet	
3	Evidence of regular (e.g. annual) review of procedures (e.g. date of last review)	–	

## Notes

*The staff responsible for information security are .....*

*The policy was last reviewed .....*

An output of the Information Governance Toolkit is a workplan (improvement plan), however you may find it useful to complete the following template workplan to support your plans to achieve Level 2 compliance by **31st March 2011**.

Requirement	Baseline Rating	Work to be Undertaken to meet Level 2	Staff Member Responsible for Task	Pharmacy Target Date for Completion of Task
114 (information governance Lead) Page 6				
115 (information governance Policy) Page 8				
116 (Contract Clauses) Page 10				
117 (Staff Training) Page 12				
118 (IGSoC Completion) Page 14				
119 (RA01 Terms) Page 16				
201 (Code of Conduct) Page 18				
208 (Mapping Flows) Page 20				
209 (Offshore transfers) Page 22				
212 (Patient Consent) Page 24				
213 (Patient Awareness) Page 26				
305 (Access Controls) Page 28				
308 (Digital Information Exchange) Page 30				
316 (Asset Register) Page 32				
317 (Physical Security) Page 34				
318 (Mobile Computing) Page 36				
319 (Business Continuity) Page 38				
320 (Incident Reporting) Page 40				

# Guide to Carrying out an IG Toolkit Assessment

Pharmacies will need to carry out the following three steps to carry out an assessment:

1. Registration of the pharmacy
2. Completion of the assessment
3. Submission of the assessment

## Step 1: Registration of the Pharmacy

A pharmacy must be registered to complete the online information governance assessment. Registration can be carried out by any individual nominated by the pharmacy. Only one registration can be made per pharmacy.

The nominated individual should select the **“Request Registration”** button from the menu of the Information Governance Toolkit (<https://www.igt.connectingforhealth.nhs.uk/>); this displays the page in **Figure 1**. All boxes need to be completed. The National Code is the pharmacy’s ODS Code (also known as the ‘F code’) which can be found at the top of the ‘Schedule of Payments’ received from NHS Prescription Services. Once this is done press the **“Next”** button at the bottom of the form to confirm all of the information is correct. If you spot any errors, please notify the helpdesk immediately (0113 394 6540).

Please ensure the email address is correct as this is how NHS CFH will contact the nominated individual with information about the Information Governance Toolkit.

**PLEASE NOTE: registration only needs to be carried out once.**

A login name and password will be sent to the email address on the registration form. Once the login and password has been received, the user should log into the Toolkit and use the **“My Password”** facility on the menu to change the password. The screen in **Figure 2** will be displayed. Complete the required fields in compliance with the **“Rules for entering passwords”** detailed on screen, then click **“Change Password”**. A message will be displayed informing the user that the password has been changed. Log out of the Information Governance Toolkit and log back in using the new password.

If there is a change of ownership and the pharmacy ODS code stays the same, the new owner should contact the Exeter helpdesk (01392 251289). The account of the previous owner can be locked and the new owner registered against that ODS code.

## Step 2: Completing the Assessment

Information is added to the assessment by:

- (a) Logging into the Information Governance Toolkit (using the new password) and selecting the **“Requirements”** button from the menu: This brings up the list of information governance requirements.
- (b) Click on a requirement to open it: This reveals a screen similar to **Figure 3** below, and contains the requirement question, the attainment levels and three blue hyperlinks titled **“Screen version”**, **“Printable version”** and **“Guidance Document”**. Click the Screen Version or Printable Version link for advice on how to assess your pharmacy’s level of compliance. Click the Guidance Document link for information on how to achieve each attainment level and links to legislation, government and national guidance, and examples of good practice from other organisations. The guidance online is in line with the guidance in this workbook.
- (c) For each requirement, enter a **“Current Rating”**, enter a **“Target”**

Figure 1

Figure 2

**Information Governance Toolkit**

My Password

Current Password:

New Password: (Case sensitive)

Confirm New Password:

**Rules for entering passwords are as follows:**

- Must be at least 6 characters long.
- Must contain both numeric and alphabetic characters.
- Should not contain dates.
- Should not contain the organisation name.
- Must not be the same as the Organisation Code or your Login ID
- Must not contain 2 consecutive identical characters. For example, the password LOOK7884 would be invalid as it contains the same character "O" side by side, or consecutively.
- Must not be a password previously used within the last year.

Getting Started  
What's New  
Requirements  
KnowledgeBase  
Reports  
My Reports  
Assessments  
My Organisation  
My Details  
My Password  
Help  
KnowledgeBase Archive

NHS 0845  
Direct 4647  
nhs.uk

Figure 3

Are pharmacy staff members provided with awareness and training across the IG agenda?  
Full details for this requirement [Screen Version](#) [Printable Version](#) [Guidance Document](#)

Requirement Attainment Levels	Current Rating	Target Rating	Past Rating
<b>Attainment Level 0</b> Staff are not aware of IG procedures and no training to address this has been implemented.	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Attainment Level 1</b> The pharmacy has a formal targeted Information Governance training programme for key staff members.	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Attainment Level 2</b> The pharmacy has in place a clear and communicated process for making all relevant staff aware of available training and ensures that all staff members who have access to confidential information are given the opportunity and actively encouraged to undertake IG training.	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Attainment Level 3</b> The pharmacy has a formal targeted Information Governance training programme which all staff must undertake on a compulsory basis.	<input type="checkbox"/>	<input type="checkbox"/>	

Estimated Date For Achieving Target Rating: (dd/mm/yyyy)

Notes/Comments:  
[View Comments From Previous Assessments](#)

KnowledgeBase  
Reports  
Assessments  
My Organisation  
My Details  
My Password  
Help  
KnowledgeBase Archive

National Information Governance Board  
NHS 0845  
Direct 4647  
NHS choices  
DH Department of Health

Figure 4

You are here: [Assessments](#) - gptest6

**Information Governance Toolkit**

Assessments  
Existing/Previous Assessments

Assessment Ref: ASS:4480

Description:  
Version 4 Assessment for General Practice Test Account (gptest6)

Requirements: Version 4

Confirmed: 14 out of 14 (100%)

Completed: 14 out of 14 (100%)

Answered: 14 out of 14 (100%)

Not Answered: 0 out of 14 (0%)

Marked Not Relevant: 0 out of 14

[View Requirements](#)  
[Implementation Plan](#)

Status	Date	User	
Started	16/03/2009 16:08:22	Ifeoma Nwolie (NHSCFH/iftw)	Assessment was unsubmitted
Submitted	02/10/2008 15:52:37	magi nwolie (gptest6/manw)	
Started	25/06/2007 09:07:37	magi nwolie (gptest6/manw)	Created automatically

Getting Started  
What's New  
Requirements  
Views  
KnowledgeBase  
Reports  
Assessments  
Organisation Admin  
My Details  
My Password  
ISO/IEC 27002:2005  
Help  
KnowledgeBase Archive  
Information Mapping

**rating** for improvement (where necessary) and set a date by which the target level will be achieved. Please also enter a comment to support your score, e.g. where evidence is held; justification for scoring a requirement is not relevant. As you update each requirement, click the **"Save Rating"** button. Alternatively the record will also save by clicking 'next'.

It may be helpful to complete 'Appendix 1' with details of the pharmacy's current rating to then transcribe into the Toolkit. In 2009/10 the target rating for pharmacies for all requirements is a minimum of **Level 2 by 31st March 2011**.

### Step 3: Submitting the assessment

Once you are satisfied that the scores recorded accurately reflect the pharmacy's level of compliance with the information governance requirements, you should select the "Assessments" option (on the menu) and then click the "Submit" button – see Figure 4.

**Note it is not possible to withdraw a submission so make sure the scores accurately reflect the assessment status of your pharmacy before clicking the submit button.**

Otherwise, any improvements in scores should be entered in the next version of the Information Governance Toolkit.

If a genuine error has been made the user should contact the Helpdesk at [pharmacy.assurance@nhs.net](mailto:pharmacy.assurance@nhs.net) or **telephone 0113 394 6540**. The request will be considered by the Digital Information Policy team, but generally a submitted assessment would only be deleted after the deadline if there are extenuating circumstances.

Once they have been submitted, the assessment and requirements can still be viewed from the assessment screen whilst a user is logged into the Toolkit.

In the unlikely event that an assessment needs to be deleted it can be done by clicking the delete button on the **"Assessments"** page and ticking the confirm deletion box. This can only be done if the assessment has not already been submitted. **Please note:** if the assessment is deleted all requirements answered and scores entered will be lost and a new assessment will have to be created.

**Take care not to delete an assessment by accident.**

### Multiples

Currently each pharmacy premises needs to be registered individually; the online Information Governance Toolkit does not support bulk-registration. Also it is not possible for a Head Office staff member to centrally view the submissions of individual stores through a central log-in, the only way for a pharmacy staff member to view a store's submission would be by logging into the Toolkit using the user name/password registered to that

store. It is hoped that functionality to support multiple Head Offices in monitoring submissions by their stores will be added in a later release of the Toolkit.

### Information Governance Toolkit Version 8

A new release of the online Information Governance Toolkit is expected in mid-2010 with enhanced functionality and improved layout. The DH Informatics Team will be working to ensure the user's guide on the site is kept updated as changes are made.

### Help

Support in registering and using the toolkit is available from NHS Connecting for Health at: **pharmacy.assurance@nhs.net** or **telephone 0113 394 6540**.

If the user of the toolkit is leaving or has left the pharmacy, please ensure that the Helpline is contacted so that another user can be registered to use the toolkit.

## Role of the PCT in Supporting Pharmacies

### Supporting pharmacies

PCTs should consider how they can best support local pharmacies to meet the information governance requirements. They may find it helpful to meet with local LPCs to identify the support that could be provided. Such support could include: arranging meetings with pharmacy information governance Leads, providing information for pharmacy information governance Leads on request, describing any specific local issues and responding to queries from pharmacy information governance Leads.

### Being a point of contact for information governance Leads

PCT staff responsible for supporting pharmacies with information governance issues should circulate their contact information to all local pharmacies. Likewise, as PCTs will find it useful to maintain a list of pharmacy information governance Leads for support purposes, pharmacies may wish to provide the PCT with the pharmacy information governance Lead's contact details.

### Overseeing pharmacy work plans

PCTs will want to work with local pharmacies to help them understand the requirement to complete an online baseline assessment against the requirements of the Information Governance Toolkit by 31 March 2010.

As pharmacies develop their work plans and document actions that need to be taken in order for them to meet the Level 2 requirements by 31 March 2011, PCTs will want to ensure that the work plans represent an honest appraisal of the pharmacy's current compliance with the information governance requirements and that they detail the appropriate steps that need to be undertaken in order for the pharmacy to meet the Level 2 requirements by the deadline.

PCTs may wish to assure themselves that pharmacies are progressing the actions identified in their work plans during 2010 as this may help to provide tailored support to pharmacies that require this. In order to do so, they may find it appropriate to visit the pharmacy. In these circumstances the

same rules for contract monitoring visits would apply (for example, the pharmacy may want an LPC representative to be present during the visit and the visit should be planned). In addition, PCTs should note that pharmacies will be unable to share patient personal information with PCT staff without patient consent and that pharmacies are not required to share commercially sensitive information.

Following a pharmacy's completion of Level 2 requirements in the Information Governance Toolkit, its PCT will wish to assess its compliance against the requirements. The evidence suggestions in this workbook will allow pharmacies to demonstrate their compliance and PCTs may wish to visit the pharmacy to undertake this assessment (which could occur as an adjunct to a formal contract monitoring visit).

### Notes

*The PCT IG lead is .....*

*Contact Details .....*

## Briefing: Confidentiality and the Law

There are a range of legal and ethical provisions that limit or prohibit the use and disclosure of personal information and, similarly, a range of provisions that require information to be used or disclosed in certain exceptional circumstances.

The privacy of personal information and personal health data are governed by the Common Law and Article 8 of the Human Rights Act 1998 (which states that “*Everyone has the right to respect for his private and family life, his home and his correspondence*”). The Data Protection Act 1998 reinforces the position through requiring all data processing to meet a range of requirements and to be lawful with extra protection for sensitive data such as health records.

All pharmacy contractors are required to comply with the NHS Code of Practice on Confidentiality and there is a professional requirement on pharmacists to comply with the RPSGB’s, “Professional Standards and Guidance” which includes references to confidentiality.

### Data Protection Act 1998

The Data Protection Act 1998 (the ‘DPA’) aims to promote high standards in the handling of personal information, and so protect the individual’s right to privacy. The Information Commissioner is responsible for enforcing the DPA.

The DPA applies to anyone holding personal information about living individuals therefore applies to all NHS community pharmacy contractors.

The DPA requires organisations to comply with a number of legal responsibilities:

- to notify the Information Commissioner you are processing personal information;
- to process the personal information in accordance with the eight principles of the DPA; and
- to answer subject access requests received from individuals.

### Notification

A notification form can be completed online ([www.ico.gov.uk](http://www.ico.gov.uk)) then printed and sent with the notification fee which is payable to the Information Commissioners Office. The notification must be renewed on an annual basis (a renewal reminder is sent out). Failure to notify is a criminal offence.

Only one notification is required per legal entity. This will cover any number of different branches or addresses where the data is processed.

In recent years, a number of private companies have been contacting businesses throughout the UK demanding fees in excess of the notification fee to register/notify your

business under the DPA. Do not be misled by these ‘agencies’. They have no official standing or powers under the DPA and there is no connection between them and the Information Commissioner’s Office.

### The Eight Data Protection Principles

The DPA places obligations on those who process information (data controllers) while giving rights to those who are the subject of that data (data subjects). Under the DPA, anyone processing personal information must comply with the eight enforceable principles of good information handling practice set out below:

#### The Eight Data Protection Principles

Data must be:

1. fairly and lawfully processed;
2. processed for a specified purpose or purposes;
3. adequate, relevant and not excessive;
4. accurate and up to date;
5. not kept longer than necessary;
6. processed in accordance with the individual’s rights;
7. protected by appropriate security (practical and organisational);
8. not transferred to countries outside of the European Economic Area without adequate protection.

Under Principle 1, at least one of the following conditions must be met for personal information to be considered fairly processed:

#### The six conditions

1. the individual has consented to the processing;
2. processing is necessary for the performance of a contract with the individual;
3. processing is required under a legal obligation (other than one imposed by the contract);
4. processing is necessary to protect the vital interests of the individual;
5. processing is necessary to carry out public functions, e.g. administration of justice;
6. processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual).

For sensitive personal information to be considered fairly processed, at least one of several additional conditions must be met. These include:

- Having the explicit consent of the individual;
- Being required by law to process the information for employment purposes;
- Needing to process the information in order to protect the vital interests of the individual or another person;
- Dealing with the administration of justice or legal proceedings.

Sensitive personal information includes health records, information on racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, sex life information, criminal proceedings or convictions.

### Overseas Data Transfers

Principle 8 of the DPA governs transfers of personal information and requires that it is not transferred to countries outside of the European Economic Area (EEA) unless that country has an adequate level of protection for the information and for the rights of individuals. The EEA is made up of the 27 EU Member States plus Iceland, Liechtenstein and Norway.



Countries outside of the EEA, known as third countries, currently deemed to have an adequate level of protection for personal data are: Argentina, Canada, Guernsey, Switzerland and the Isle of Man. Personal information can also be transferred to companies in the USA that have signed up to the 'safe harbor' agreement. These companies have agreed to abide by a set of rules similar to those found in the DPA.

More information can be found in the Information Commissioner's guidance 'Information Commissioner: The Eighth Data Protection Principle and International Transfers'.

Information about overseas transfers of information must be included within the pharmacy's data protection notification to the Information Commissioner.

Note, Department of Health guidelines on overseas information transfers are more restrictive than the DPA and these require that personal information is **NOT** transferred outside of the UK unless appropriate assessment of risk has been undertaken and mitigating controls put in place.

### The Rights of Individuals under the DPA

The DPA also enforces seven rights of individuals:

- 1. The right to subject access**  
This allows people to find out what personal information is held about them.
- 2. The right to prevent processing**  
Anyone can ask a data controller not to process information relating to him or her that causes substantial unwarranted damage or distress to them or anyone else. [Note: Although a patient could demand that there is no record made on the PMR system the Terms of Service provide a statutory requirement for the entry so the patient would have to accept that they cannot receive the NHS service (in this case the processing of personal information is warranted irrespective of any evidence the patient is able to provide of distress or harm that is being caused to them or someone else).]
- 3. The right to prevent processing for direct marketing**  
Anyone can ask a data controller not to process information relating to him or her for direct marketing purposes.
- 4. Rights in relation to automated decision-taking**  
Individuals have a right to object to decisions made only by automatic means e.g. there is no human involvement.

**5. The right to compensation**

An individual can seek compensation from a data controller for damage and distress caused by any breach of the DPA. Compensation for distress alone can only be sought in limited circumstances.

**6. The right to rectification, blocking, erasure and destruction**

Individuals can apply to the court to order a data controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion based on inaccurate information.

**7. The right to ask the Commissioner to assess whether the DPA has been contravened**

If someone believes their personal information has not been processed in accordance with the DPA, they can ask the Commissioner to make an assessment. If the DPA is found to have been breached and the matter cannot be settled informally, then an enforcement notice may be served on the data controller in question.

**Subject Access Requests**

Individuals have a right under the DPA to make a request in writing for a copy of the personal information that is held about them. This is called a subject access request. They are also entitled to be given a description of the information, its purpose, who it might be passed on to and any further information about the source of information.

Data controllers can ask for any information which they reasonably require in order to verify the identity of the person making the requests and to locate the data.

Once a request has been received, Data controllers have to provide a copy of the requested information within 40 days.

Data controllers may charge a fee of up to £10 for responding to a subject access request where information is stored on a computer. If the record consists of both a computerised and a manual record, up to £50 can be charged. If the request is not received in writing or the individual is not willing to pay the fee, it is not obligatory to provide the information.

**Human Rights Act 1998**

Article 8 of the Human Rights Act 1998 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality should satisfy Human Rights requirements.

Any decision to override a duty of confidence in the public interest must be consistent with the rights described in Article 8. This requires that any disclosure of personal information must be necessary and proportionate:

- Disclosures must be necessary to achieve the purpose (e.g. the risks of non-disclosure should be identifiable, real and arising in the foreseeable future) and limited to the relevant details. Each disclosure must be considered on its own merits.
- The public interest served by the disclosure must outweigh the competing public interest in protecting the confidentiality of the individual's health information and more generally in the provision of a confidential health service.

**Common Law Duty of Confidence**

Decisions taken by the UK courts, together with ethical duties of confidentiality placed on pharmacists and other clinical professionals, have resulted in personal health information being treated with a much higher degree of sensitivity than most other types of personal information. This has resulted in acceptance that personal health information can only be disclosed to a third party when:

- the patient provides explicit consent; or
- there is a legal requirement to do so; or
- there is an overriding public interest (for example, to prevent a serious crime from taking place).

**Confidentiality NHS Code of Practice**

The Confidentiality NHS Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations and is concerned with issues surrounding confidentiality and patients' consent to the use of their health records.

The aim of the Code is to ensure that all patient information is processed fairly, lawfully and as transparently as possible by NHS staff and contractors so that the public:

- understand the reasons for processing personal information;
- are asked for their consent for the disclosure and use of their personal information;

- gain trust in the way the NHS handles information and;
- understand their rights to access information held about them.

## NHS Pharmaceutical Regulations

The National Health Service (Pharmaceutical Services) Regulations 2005 include a number of provisions relevant to information governance including requirements on pharmacies to have;

- appropriate arrangements (having regard to issues both of rights of access to information and of confidentiality) to support both health care delivery and clinical governance,
- appropriate arrangements in respect of compliance with "Confidentiality: the National Health Service Code of Practice",
- monitoring arrangements in respect of compliance with the Data Protection Act 1998 and with regard to patient confidentiality, and
- appropriate training for staff with regard to compliance with the Data Protection Act 1998 and patient confidentiality.

More information about the NHS (Pharmaceutical Services) Regulations can be found on the PSNC website ([www.psn.org.uk/regulations](http://www.psn.org.uk/regulations)). Failure to comply with these requirements may result in a PCT taking action for breach of the Terms of Service.

## RPSGB Code of Ethics and Professional Standards

The RPSGB Code of Ethics requires that pharmacists take all reasonable steps to prevent accidental disclosure or unauthorised access to confidential information and ensure that confidential information is not disclosed without consent, apart from where permitted to do so by the law or in exceptional circumstances. The RPSGB standards for patient confidentiality can be accessed online at: <http://www.rpsgb.org/pdfs/coepsgpatconf.pdf>. Failure to adhere to these standards could form the basis of a complaint of professional misconduct.

## The Caldicott Principles

The December 1997 Caldicott Report identified weaknesses in the way parts of the NHS handle confidential patient data.

The report defined six Caldicott principles which provide a framework for the management of access to personal information with the NHS.

### Caldicott Principles

- |             |   |
|-------------|---|
| Principle 1 | Justify the purpose for using confidential information    |
| Principle 2 | Only use identifiable information if absolutely necessary |
| Principle 3 | Use the minimum that is required                          |
| Principle 4 | Access should be on a strict need to know basis           |
| Principle 5 | Everyone must understand their responsibilities           |
| Principle 6 | Understand and comply with the law                        |

## Deceased patients

The records of deceased patients must be treated with the same level of confidentiality as those who are living. The Access to Health Records Act 1990 governs access to the health records of deceased patients. Further information about the requirements of this Act can be found at [www.dh.gov.uk](http://www.dh.gov.uk).

## Support

Support is available through the Information Commissioner Helpline (01625 545745) and from the RPSGB Information and Advisory Service (020 7735 9141).

## Briefing: Consent and the Law

### What is Consent?

The Oxford English Dictionary defines consent as “permission or agreement”. In the healthcare context, consent is a person’s agreement to receive a treatment or professional service that is appropriate to their needs.

“The securing of consent for any health intervention, whether or not it involves physical contact, is essentially the embodiment of respect for the patient’s autonomy”

Wingfield J. “Consent: The heart of patient respect.” *Pharm. J.* (2007) 279: 411

### Why is consent important?

Administration of a treatment to a patient without their consent, involving any kind of physical contact may leave a practitioner open to a charge of battery (non-consensual physical contact) or negligence (failure to inform the patient and seek consent) under English law.

Consent extends to all decision-making about a patient’s healthcare, including the storage, use and disclosure of patient information collected to support the clinical care of the patient. The NHS Confidentiality Code of Practice stipulates that patients should give their consent for the disclosure and use of their personal information by health professionals. Consent can be implied where the disclosure is to other healthcare professionals involved in the patient’s care; other disclosure will require the patient’s explicit consent.

Under the Data Protection Act 1998, the pharmacy contractor is the data owner, and eight general data protection principles apply (discussed in detail in previous section on Confidentiality and the Law). For the first of these, that data are fairly and lawfully processed, consent is one of the conditions that can evidence the processing being done is fair and lawful.

### What is valid consent?

Consent may be implied or explicit. **Implied** consent is where the patient indicates their consent by their action. For example, when a patient hands a prescription form in at the pharmacy, they are giving implied consent for the pharmacy staff to dispense the prescription. **Explicit** consent is where the patient actively indicates their consent, either verbally, or in writing (by completing and signing a form).

For consent given to be valid, the following criteria must apply:

1. The patient must have the capacity to make the decision in question, and to understand the information provided during the decision making process.

2. The patient must be given sufficient information to be able to make an informed decision about the service they are being offered.
3. The patient must make the decision voluntarily, i.e. they must not be coerced or put under pressure to make a certain decision.

### Capacity

Adults over the age of 18 are presumed to have capacity to make decisions about their healthcare. Young children and patients who have mental disorders (for example, dementia) may not have the capacity to make some decisions about their healthcare.

Pharmacists are reminded of the principle set out in the Fraser Guidelines (sometimes referred to in terms of ‘Gillick competence’) whereby a person under the age of 16 can give consent if he or she has “sufficient understanding and intelligence to enable him or her to understand fully what is proposed.”

However, in England and Wales, where young people under the age of 18 refuse to give consent, their decision may, in exceptional circumstances, be overridden by the courts, where this is considered to be in the young person’s best interests.

Traditionally, assessment of a patient’s capacity to give consent for a treatment has been left to the discretion of





Steve Cole/Stock

the practitioner, based on his or her experience and judgement. Recently, the concept of capacity has become more well-defined legally due to case law, and the Mental Capacity Act 2005 has established principles and safeguards for vulnerable adults.

The principles of the Mental Capacity Act, 2005, are as follows:

- Every adult is presumed to have capacity;
- Individuals have the right to be supported to make their own decisions;
- Individuals retain the right to make what might be seen as eccentric or unwise decisions;
- Interventions for people without capacity must be the least restrictive possible;
- Any action taken on behalf of a person without capacity must be in their best interest (not that of the health professional or their organisation).

### Informed Consent

The pharmacist should ensure that the patient has sufficient information (clear, accurate and presented at a level that the person can understand) to make the decision in question. Care should be taken to address any particular communication needs (poor sight/hearing, or a language barrier), and the person's understanding of what has been asked should be confirmed.

Pharmacists should bear in mind that research indicates that the explanation given (appropriate level of detail,

quality of communication etc.) has a bearing on the likelihood of consent being given.

### Voluntary Consent

The patient's consent should be given voluntarily and without any coercion. Pharmacists should bear in mind that some people may adopt inappropriately passive roles if they are distressed or in pain.

Pharmacy staff should never put pressure on patients to provide information or to give consent for information to be shared, in order to meet commercial objectives and targets in service development.

Another important aspect of voluntary consent is that the patient should be able to change their mind at any time about the treatment or service being offered, and rescind the consent they have given.

### Obtaining Consent to Store Information about Patients

In accordance with the Data Protection Act 1998, pharmacies are required to obtain a patient's consent to store information about them to support services provided, stating the purpose for which the information is being collected.

However, the NHS (Pharmaceutical Services) Regulations 2005 require pharmacists to keep and maintain records of drugs and appliances provided and also of advice given and any intervention or referrals made. In these cases, because the legislation requires the record, patient consent is not required to store and maintain the record, but patients should be made aware that records are being kept for them and the purpose for which the records are used (see Information Governance Requirement 213). If patients refuse consent they should be advised of the consequences of being unable to access the NHS pharmaceutical service.

A pharmacy should seek explicit, informed consent from a patient to process information, including storing personal data to support those pharmacy services where the keeping of records is not mandated in statute. For example, patient's consent is required to share personal information linked to the delivery of a local enhanced service with the patient's prescriber.

The Royal Pharmaceutical Society's Professional Standards and Guidance indicates that obtaining consent is an ongoing process not a single event. Consequently, as well as obtaining consent when the service is offered to patients, pharmacies should, where practical, review the patient's consent when there are significant changes to the service being offered.

In the context of collecting information from a patient to support a service, this might include:

- If the patient's circumstances change;
- If new information is required from the patient to provide the same service;
- If the procedure for service provision changes;
- If the patient data needs to be stored in a different location;
- If a change in procedure requires routine disclosure of information to a third party in order to provide the service;
- If a third party requests disclosure of information for a particular patient.

Pharmacists should ensure that they have a standard operating procedure (SOP) for obtaining consent from patients to collect and store information to provide pharmacy services.

### Information Sharing

Disclosure of patient information without the subject's explicit consent other than where consent is implied or there is a specific exception (see below) generally constitutes a breach of the Data Protection Act, 1998, as well as of the common-law duty of confidence.

The Royal Pharmaceutical Society's Professional Standards and Guidance on Patient Confidentiality indicate that:

*"Patients will generally expect that information you obtain in the course of your professional practice may be shared with other healthcare professionals or others who have a duty of confidentiality, where necessary for their care."*

This will be most evident where there is a shared care arrangement, for example where the pharmacy is providing services to patients in the course of a clinic organised with the local surgery. When dispensing a prescription the pharmacist would be expected by the patient to discuss the treatment with the GP if this is going to ensure patient safety.

In some cases, sharing will require explicit consent such as Medicines Use Reviews (MURs) where the Secretary of State Directions require the patient's consent to share MUR information with the patient's prescriber.

### Disclosure of Information without Patient Consent

Pharmacists have a duty to safeguard personal data and not to disclose patient data to a third party without the subject's consent. Unauthorised disclosure of patient identifiable data collected under the Data Protection Act

1998 (disclosure without the patient's consent) constitutes a breach of the Act.

There are a few exceptions to this, where disclosure may be made without the patient's consent:

- Where the patient's parent, guardian or carer has consented to the disclosure and the patient is deemed by law to be, or appear to be, incapable of consenting;
- Where disclosure is to a person or body empowered by statute to require disclosure of that information;
- Where disclosure is directed by HM Coroner, a judge or presiding officer of a court, Crown Prosecution Office in England or Wales, or Procurator Fiscal in Scotland;
- Disclosure to a police officer or NHS fraud investigation officer who provides, in writing, confirmation that disclosure is necessary to assist the prevention, detection and prosecution of serious crime;
- Where necessary to prevent serious injury or damage to the health of a patient, a third party or to public health;
- Where disclosure is necessary for the protection of children or vulnerable adults.

Before releasing information about a patient without the patient's consent, pharmacists should, where possible, endeavour to persuade the patient to release the information themselves for the purpose for which it is required, or to give their consent for the information to be released, unless consulting the patient would itself hinder or defeat the purpose of the disclosure. The reasons for disclosing personal information without consent should be fully documented in all cases.

Where records are deliberately accessed without authority, the individual may face criminal charges. Pharmacists and pharmacy technicians may also face disciplinary action by the Royal Pharmaceutical Society for a breach of professional standards.

### References

- 1) Wingfield J. *Consent: the heart of patient respect*. *Pharm J* (2007) 279: 411-414
- 2) *Professional Standards and Guidance on Patient Consent*. Royal Pharmaceutical Society of Great Britain.
- 3) *NHS Confidentiality Code of Practice*

## Guidance on Specific Data Transfer Routes

### Physical Transfer

#### Using postal/courier services

Hardcopy documents are still routinely used in pharmacies, for example prescription forms, MUR forms and forms linked to local enhanced service provision.

The Drug Tariff (Part II Clause 5) requires that prescriptions being sent to NHS Prescription Services for reimbursement are sent in a secure manner that enables tracking and tracing of the delivery.

For other information, it would be for the pharmacy contractor to decide, based on a risk assessment, whether information should be sent by post or courier, for example based on the volume and sensitivity of information being sent.

### Verbal Communications

The security and confidentiality of telephone and personal conversations should be considered within the pharmacy's code of practice on confidentiality as well as SOPs and staff training.

#### Recorded messages

Recorded telephone messages may contain personal or sensitive information such as names and addresses of patients phoning about prescriptions, details of health professionals phoning with queries about patients or applicants for jobs advertised.

Consideration should be given to which staff members have access to answering machines. Password protected voicemail boxes can be used to control access where this functionality is available on the phone.

Some pharmacies use a messages book to record messages; care should also be taken to ensure this is stored appropriately.

#### IP Phones

IP phone systems use voice over IP technologies to allow telephone calls to be made across an internet connection rather than via standard telephony.

IP phones are subject to similar security risks to unsecured email, for example 'eavesdropping', 'traffic sniffing' and 'unauthorised re-routing'.

The level of risk will depend on the size and architecture of the IP phone deployment and pharmacies wishing to implement this technology to transfer personal or sensitive data should seek expert advice from an appropriate information security professional.

### Fax Communications

Fax communications are routinely used in pharmacies – for example, to receive copies of urgently-required FP10 prescription forms, discharge communications from secondary care and to support communication with care homes.

Best practice in sending and receiving faxes is:

- 1) The sender to phone the recipient to advise them that a fax is about to be sent.
- 2) The sender should double-check the fax number and, where possible, use fax numbers that are pre-programmed into the fax machine. Note some NHS organisations have a fax machine designated to be used for confidential information.
- 3) The fax should be sent with a cover sheet stating who it is intended for, and marked "Private & Confidential" to a named recipient.
- 4) The sender should ensure the original document is removed from the fax machine.
- 5) The recipient should remove the fax from the machine on receipt.
- 6) The recipient should contact the sender to confirm receipt and that the fax will be appropriately dealt with and safely stored.

In pharmacies, if the fax machine is receiving personal information, it should be sited in a 'safe haven', for example the dispensary, where access to the machine is controlled.

#### eFax

eFax software allows users to send or receive a fax via a computer rather than a fax machine. The information governance risks for eFax are therefore a combination of the risks linked to email and standard fax communications.

There is currently no eFax service recognised as being sufficiently secure to support the routine transfer of patient personal data.

### E-mail Communications

NHSmail is currently the only NHS approved method for exchanging patient data by email, but only if both sender and recipient use an NHSmail account or if sending to another government secure domain such as:

- GSi (\*.gsi.gov.uk)
- CJX (\*.police.uk or .pnn.police.uk)
- GSE (\*.gse.gov.uk)

- GSX (\*.gsx.gov.uk)
- GCSX (\*.gcsx.gov.uk)
- SCN (\*.scn.gov.uk)
- CJSN (\*.cjsn.net)
- MoD (\*.mod.uk)

Other email services should not normally be used for sending personal or sensitive information.

Work is ongoing to facilitate an NHSmail address for all pharmacies and community pharmacy staff that require one. More information about NHSmail for pharmacy staff is available on the PSNC website ([www.psn.org.uk/nhsmail](http://www.psn.org.uk/nhsmail)).

Where NHSmail is used to send sensitive information, this should be clearly indicated in the subject header, for example marked 'Confidential'.

One interim option for pharmacies that do not yet use NHSmail is to transmit personal information as an encrypted attachment. The NHS recommendation is for AES256 encryption to be employed. This standard is available when using applications such as PGP or WINZIP version 9 or above. With these products the data can be put into a Self Decrypting Archive (SDA). The sender should check beforehand that the recipient also has WinZip and therefore will be able to de-encrypt the attachment. The pass phrase for the archive must be of an appropriate length and complexity and to ensure the safety of data in transit the pass phrase should be communicated to the recipient separately from the encrypted data so that the intended recipient is the only one able to decrypt the data. As well as software requirements, consideration would also need to

be given to staff training and the workload involved in creating, opening and decrypting an archive. Care would need to be taken to ensure no sensitive information is included in the email itself.

When emails including attachments are received containing personal or sensitive information, either via NHSmail or encrypted attachments from other email solutions, they should be stored appropriately on receipt, for example incorporated into the health record and deleted from the email system when no longer needed.

Some companies monitor emails for malicious codes or misuse. Where this is undertaken, organisation email and internet policies should include guidance for staff on what monitoring is being routinely conducted. Comprehensive guidance is available in the Employment Practices Code which has been produced by the Information Commissioner's office.

### SMS Text Messages

There are various potential applications for text messages in the provision of pharmacy services, for example patient reminders to collect prescriptions or attend an appointment for an MUR.

Key considerations when using text messages are:

- 1) Is the mobile phone number correct?
- 2) Is the mobile phone receiving the text message being used by the intended recipient of the message?
- 3) Has the message been received, and what provision is there to audit message receipt?
- 4) Text messages are normally stored on SIM cards and are typically only cleared when overwritten (not necessarily when erased) - as mobile phones are easy to misplace or may get stolen, there a danger of a breach of confidentiality occurring that the patient may find embarrassing or damaging.

Text messages should not normally be used to convey sensitive information, for example test results, and the use of text messages for the transfer of personal data should be kept to a minimum. For example, a reminder to collect a prescription does not need to include the name of the medication.

Pharmacists should carefully weigh the benefits of using text messages to convey patient information against the risks of doing so.

When consent is sought for patient reminder services, patients should be informed of what information will be included in standard SMS messages sent to them via the service.



### **Electronic Messaging Software**

Electronic instant messaging (IM) software, such as MSN Messenger and Yahoo! Messenger presents a number of information governance risks to users:

- 1) IM software is particularly vulnerable to malware, such as virus, Trojans and worms.
- 2) In many IM services, data is unencrypted. Such services therefore do not provide sufficient security for transmission of patient data, as they are at risk of unauthorised access and electronic surveillance.
- 3) In many IM services, there are no audit trails of access and transmission. The NHS Care Records Guarantee has a requirement for systems to maintain audit trails for the access and transmission of patient data.
- 4) IM services can be used to bypass restrictions on what can be sent as e-mail attachments.

IM software is therefore not suitable for use for the transmission of personal data.

Whilst it is possible that solutions will be developed in future which offer the necessary security and audit controls, there are no IM solutions currently recognised by the NHS as being suitable for transmission of personal information. Pharmacies wishing to implement this technology to transfer personal or sensitive data should seek expert advice from an appropriate information security professional.



### **Web Applications**

There are a number of web applications that collect and transfer sensitive or personal information, for example online platforms to support the recording of local enhanced services and internet pharmacy portals used to collect patient information and requests via the internet.

Pharmacy contractors should satisfy themselves that applications used to support the delivery of NHS services comply with the NHS Code of Practice on Confidentiality and have appropriate information security measures in place to prevent unauthorised or unlawful processing or accidental loss, destruction, or damage of personal information.

### **Remote Desktop Access Software by Pharmacy Staff**

There are a number of commercially available remote access solutions that provide an instant secure connection from one PC to another across the internet. For example, this could be used to provide access to a computer in a GP practice from within the pharmacy or it could be used by a pharmacist with a wireless internet solution undertaking a service outside the pharmacy to remotely access records within the pharmacy.

NHS CFH has opted not to approve any remote connection providers but some solutions have been given support by certain PCTs. If using a remote access solution, pharmacy contractors should satisfy themselves that applications comply with the NHS Code of Practice on Confidentiality, seeking expert advice where necessary.

### **Virtual Private Networks**

Some pharmacies may wish to create Virtual Private Networks (VPNs) within their business, for example to allow the Head Office secure access to a computer in a particular branch. Expert advice on VPNs should be sought from pharmacy system suppliers.

### **Portable Data Storage Devices and Mobile Computing Devices**

Portable data storage devices, such as data sticks (also known as USB sticks or pen drives) and also mobile computing devices such as laptops and PDAs, are often used in pharmacies.

Best practice requires that personal or sensitive data should only be held on portable data storage devices when it is essential to patient care, and if so, should be encrypted, according to NHS data standards. In addition, the device should be protected by a strong and secure password.

It is recognised that for some devices such as laptops, encryption may take some time to achieve. Therefore, if following a risk assessment it is felt that continued reliance upon unencrypted data is necessary for the benefit of patients, the outcome of the risk assessment must be reported to the most senior person in the pharmacy, so that he/she is appropriately accountable for the decision to accept data vulnerability or to curtail working practices in the interests of data security. Expert guidance on encryption of computers should be sought from system suppliers.

### NHS Encryption Standards

The NHS information governance data encryption algorithms currently applicable are 3DES, AES 256 or Blowfish. These algorithms should be used with a recommended minimum key length of 256 bits where available.

Secure memory sticks that comply with NHS standards (e.g. 256-bit AES256 hardware encryption) are now freely available to buy off-the shelf from IT retailers. Some devices automatically enforce formation of a strong and therefore more secure password. An alternative option to using an encrypted memory stick is to encrypt the file itself held on the memory stick. The NHS recommendation is for AES256 encryption to be employed. This standard is available when using applications such as PGP or WINZIP version 9.

If portable data storage devices are being transferred between sites or organisations, for example data sticks with MUR or other patient records; they should be properly packaged and clearly labelled to ensure they are handled correctly. The password should be transferred separately to the device, e.g. if the device is posted, the password should be sent in a separate envelope or communicated through a different route such as by phone.

No more than the minimum amount of data needed to support the work being done should be stored on a portable storage device.

The greatest security risk with portable devices is the loss or theft of the device itself. Users should therefore:

- 1) Keep devices in a safe and secure place, wherever they are being used.
- 2) Ensure appropriate encryption is applied to the device or the data.
- 3) Report loss, theft or suspected unauthorised disclosure of data immediately.



- 4) Consider remote data wiping functions for PDAs and mobile phones.
- 5) Not store devices and access tokens in the same location.

### Wireless Networks

There is an emerging use of wireless networks within community pharmacies, for example to support connecting laptops in a consultation area to the pharmacy network without the need for cabling. Expert advice (e.g. from pharmacy system suppliers) should be sought to set up a wireless network in a community pharmacy. Some suppliers have chosen not to support or endorse wireless networks.

## Guidance on Data Mapping and Risk Assessment

A key requirement of information governance assurance is to map and record all routine flows of personal information (Requirement 208). This is then used to identify risks associated with data transfer so that appropriate measures can be taken to remove or mitigate the risks.

### Step 1: Mapping Flows

Only routine (including annual) flows of sensitive or personal information should be considered in the mapping exercise (i.e. flows that occur on a regular basis). Bulk data flows, in particular, should be mapped.

There are four elements to consider for every transfer:

- 1. Data Items:** the information being transferred, for example, an MUR form, prescription information, enhanced services information;
- 2. Format:** for example, hardcopy MUR form, hardcopy prescriptions, email or information uploaded to online systems that collect information such as websites to support the delivery of enhanced services;

- 3. Transfer Methods:** for example post, fax or email. National NHS Applications such as EPS can be excluded.
- 4. Location of the recipient,** for example NHS Prescription Services, the GP surgery or PCT office. It is not necessary to give a name to every single location if the same data format and transfer method are used, for example if the pharmacy sends MUR forms to local GP surgeries, there is no need to list the address of every GP surgery.

A template information flow map for a pharmacy can be found on page 60. This should be locally tailored.

### Step 2: Identifying and Categorising Risks

It is important that any risks in transferring personal or sensitive information are identified as a result of the mapping process. The table below provides a method of allocating a basic grading system of 'High', 'Medium' or 'Low' to the security risk afforded by a particular transfer method. It compares the impact of data loss, for example the impact on patients and the pharmacy business and cross references this with the likelihood of data being lost.

#### Categories of Risk

IMPACT	LIKELIHOOD				
	Probable	Possible	Unlikely	Rare	Negligible
Critical	HIGH	HIGH	HIGH	MEDIUM	LOW
Major	HIGH	HIGH	MEDIUM	MEDIUM	LOW
Moderate	HIGH	MEDIUM	MEDIUM	LOW	VERY LOW
Minor	MEDIUM	MEDIUM	LOW	LOW	VERY LOW
Insignificant	LOW	LOW	VERY LOW	VERY LOW	VERY LOW

#### Impact definitions / Incident Classification

This impact classification system can also be used to classify information security incidents (requirement 320).

Insignificant:	Minor:	Moderate:	Major:	Critical:
Minimal discernible effect on patients or the pharmacy.	Minor breach, for example data lost but files encrypted, less than five patients affected.  <i>Inconvenient to the pharmacy but manageable.</i>	Moderate breach, for example unencrypted clinical records lost, up to 20 patients affected.  <i>Potential for damage to the pharmacy's reputation.</i>	Serious breach, for example unencrypted clinical records lost, up to 1,000 patients affected or particular sensitivity e.g. sexual health information disclosed.  <i>Potential for damage to the pharmacy's reputation and/or local media coverage.</i>	Serious breach in terms of volume of records, for example over 1,000 patients affected or particular sensitivity of records.  <i>Damage to the reputation of the NHS and the pharmacy profession. Potential for national media coverage.</i>

**Guidance on key risk factors:**

<b>Data Flow Attributes</b>	<b>Guidance</b>
<b>Is the data bulk data? (concerning 51 or more subjects)?</b>	Bulk data transfer carries a higher risk than individual data transfer
<b>Is the data sensitive data?</b>	Sensitive data transfer carries a higher risk than transfer of other types of data
<b>Is the data going outside of the pharmacy premises and/or the pharmacy organisation?</b>	Data going outside the pharmacy premises and organisation carries a higher risk than data remaining in the pharmacy premises
<b>Is the data being transferred overseas?</b>	Transfer out of the UK and the European Economic Area carries a higher risk than transfer to another location in the UK
<b>What is the method of data transfer?</b>	<ol style="list-style-type: none"> <li>1) Automatic system transfer is high risk if via an insecure network</li> <li>2) Courier transfer is high risk if pharmacy does not have a contract with courier company</li> <li>3) E-mail is high risk, but can be reduced if sender and recipient use NHSmail, OR use alternative encryption that meets the NHS IG standard, AND confirmation of recipient's address</li> <li>4) Fax is high risk if safe haven is not implemented</li> <li>5) Hand deliveries are high risk due to risk of loss (if a removable storage device is used it must be encrypted to reduce the risk)</li> <li>6) Post – risk reduced by use of a) sealed envelopes, b) track &amp; trace postal services. (If a removable storage device is used it must be encrypted)</li> <li>7) Text messages are high risk (use only for non-sensitive data)</li> </ol>

**Step 3: Recording Risks**

A record of risks is commonly referred to as a 'risk register'. All information governance risks identified in step 2 should be recorded in an information governance risk register.

The table on page 61 could be used as the pharmacy's risk register. This should be localised as appropriate.

**Step 4: Reporting and Mitigating Risks**

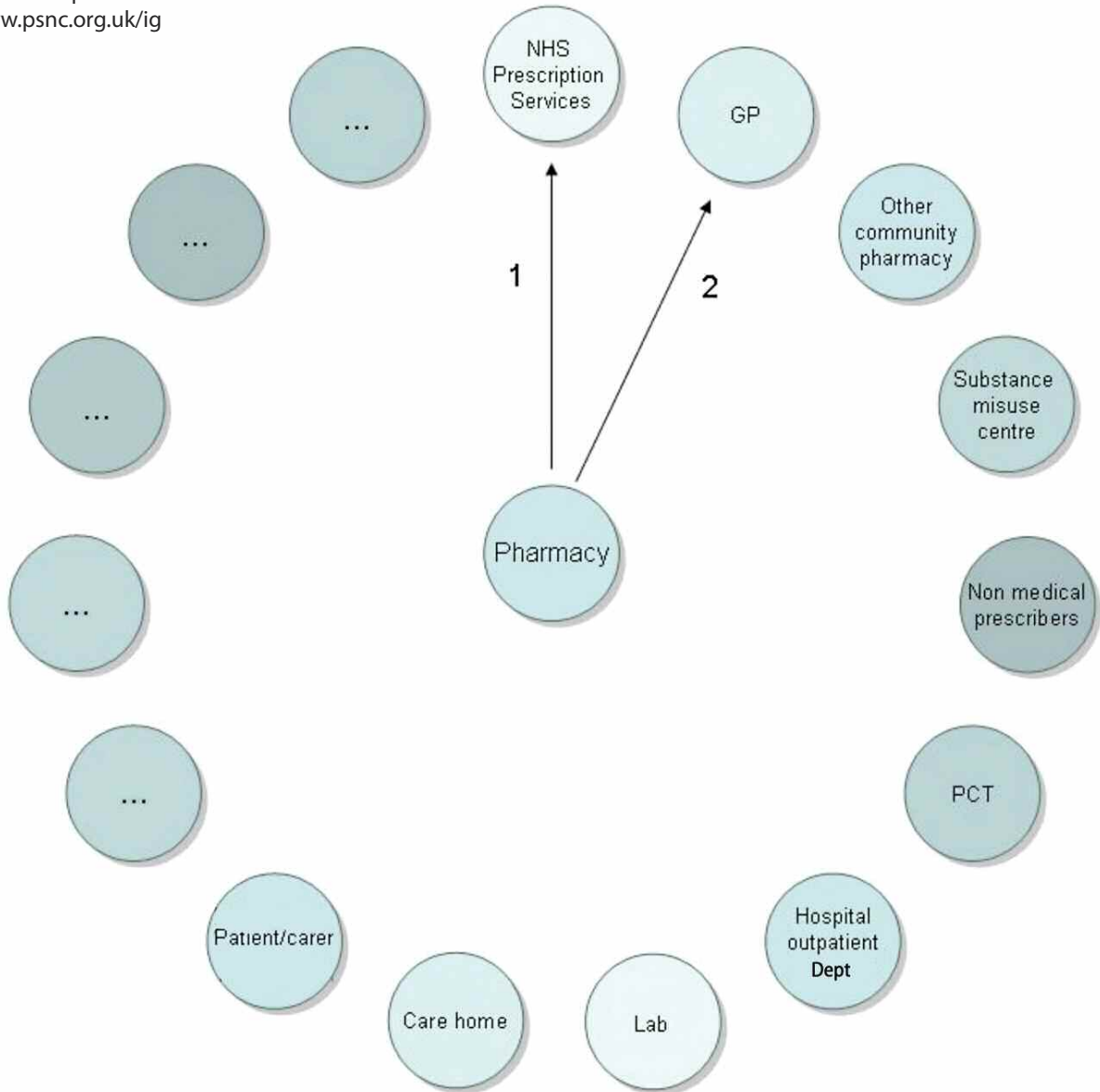
In some circumstances, the necessities of patient care may justify a degree of risk for a period, but where possible, plans should be developed for securing the data flow as soon as possible.

Where significant risks are highlighted by the mapping exercise, immediate action should be taken to either suspend the transfer of information until remedial action can be taken, or to transfer the information by another, more secure method.

Any significant risks should be reported by pharmacy staff to the pharmacy's information governance Lead.

### Pharmacy Map of Information Flow

Draw arrows on the diagram below to indicate the direction of information flow between the pharmacy and external organisations. Use the blank headings to add details of any organisations you exchange data with it that are unique to your pharmacy. Worked examples can be found online at: [www.psn.org.uk/ig](http://www.psn.org.uk/ig)



**Telephone & Personal Conversations:** Mapping can only be carried out on tangible information flows and where physical evidence of the information exists. If telephone calls are recorded or discussions transcribed to tapes etc. which are then routinely sent to different locations, these will count as data flows. The security and confidentiality of telephone and personal conversations is clearly very important but must be addressed through policies, procedures and staff training. Information which flows through the NHS Care Records Service does not need to be considered as it is protected by the robust access control and confidentiality framework developed by NHS CFH.

**Transfers within a Pharmacy Company:** Transfers within a pharmacy company do not need to be documented in this mapping exercise; however pharmacy companies should ensure they meet their legal obligations including compliance with the Data Protection Act.

## Data Flow Risk Register

Describe the nature of the information flow between the pharmacy and the external organisation, e.g. data item, format, transfer method	Identify the type and risk level of breaches of confidentiality	Describe the measures taken to mitigate the risk of breaches in confidentiality of information that is passed between the pharmacy and the external organisation
<b>NHS BSA Prescription Services</b>		
1. <i>Paper prescriptions transferred by recorded delivery</i>	<i>Medium</i>	<i>Track and trace service used as required by the Drug Tariff</i>
<b>GP</b>		
2. <i>Paper Repeat prescription requests and MUR forms carried by staff to the GP surgery</i>	<i>Low</i>	<i>Staff follow data transfer process</i>
<b>Other community pharmacy</b>		
<b>Substance Misuse centre</b>		
<b>Non medical prescribers</b>		
<b>PCT</b>		
<b>Hospital Outpatient Dept.</b>		
<b>Lab</b>		



**Access controls:** a range of measures and processes that ensure entry to a computer system, network or premises is restricted to particular and authorised users.

**Aggregators:** There are two ways that pharmacies can connect to N3, either through a third party commercial network provider (also known as an 'aggregator') or a direct connection to N3. The third party providers include InTechnology, IMS Securenet and Vialtus. For business reasons, almost all pharmacies have chosen to connect via a third party provider. A number of multiple pharmacies have arranged for their corporate networks to connect to N3.

**Anonymised information:** information which does not identify an individual directly, and cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification.

**Caldicott Guardian:** a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. Pharmacies are not required to appoint an internal Caldicott Guardian.

**Encryption:** putting data into a secret code so it is unreadable except by authorised users.

**Malicious code:** software capable of performing an unauthorised process on an information system.

**Memory sticks:** an extremely compact and portable form of digital storage (approx 1" x 2") that come in various capacities.

**NHS CRS:** The NHS Care Records Service (NHS CRS) is a secure service that links patient information from different parts of the NHS electronically so authorised NHS staff and patients have the information they need to make care decisions. There are two elements to the NHS CRS; detailed records (held locally) and the Summary Care Record (held nationally). There are a number of supporting components including the Personal Demographics service which holds non-clinical demographics information.

**Personal information:** also referred to as, "personal identifiable information/data" and relates to information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

**PDA:** A Portable Digital Assistant (PDA) is a mobile computing device which can be used to capture data and/or allow convenient access to reference material. PDAs vary in additional functionality for example some can be used as mobile phones and provide access to the internet.

**Pseudonymised information:** data that have been given unique identifier or random code in order to break the link to the data subject.

**RA01 form:** the document containing the conditions a successful applicant has to agree to before becoming an authorised NHS Care Records Service user and being issued with a Smartcard.

**Safe haven:** a term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the safe haven principles.

**Sensitive data/information:** a category of personal information that is usually held in confidence and whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community, e.g. health records, sexual orientation information.

<i>Organisation</i>	<i>Contact Information</i>	<i>Type of Support</i>
<b>DH Informatics Helpdesk</b>	Email: <a href="mailto:pharmacy.assurance@nhs.net">pharmacy.assurance@nhs.net</a> Tel: 0113 394 6540. Web: <a href="http://www.igt.connectingforhealth.nhs.uk/">www.igt.connectingforhealth.nhs.uk/</a>	General guidance on the requirements and technical support in using the Information Governance Toolkit.
<b>PSNC Information Team</b>	Email: <a href="mailto:info@psnc.org.uk">info@psnc.org.uk</a> Tel: 01296 432823 (Option 1) Web: <a href="http://www.psn.org.uk/IG">www.psn.org.uk/IG</a>	General guidance on the requirements.
<b>Information Commissioner's Office</b>	Tel: 08456 30 60 60 Web: <a href="http://www.ico.gov.uk/">http://www.ico.gov.uk/</a>	Guidance on the Data Protection Act.
<b>PCT</b>	Your LPC or PCT pharmacy support staff should be able to put you in contact with the PCT information governance Lead.	Additional support in working through some of the requirements may be available locally.
<b>RPSGB Information and Advisory Service</b>	Tel: 020 7735 9141	General guidance on issues related to confidentiality and consent.

This resource has been produced by the PSNC and the Royal Pharmaceutical Society of Great Britain with the support of the Department of Health, NHS Connecting for Health and NHS Employers. Comments and suggestions on how to improve the guidance are welcomed and should be directed to [info@psnc.org.uk](mailto:info@psnc.org.uk). Alternatively, contact the PSNC Information Team on 01296 432823.

© PSNC. If you wish to reuse sections of this guide please send a request to [info@psnc.org.uk](mailto:info@psnc.org.uk)

For any pharmacist, understanding IG will be relevant CPD. Why not make a record in your RPSGB CPD Plan & Record file or online at [www.uptodate.org.uk](http://www.uptodate.org.uk)

