

NHS Information Governance: 2010/11 UPDATE



JANUARY 2011



Contents

- Outline of the Changes
- Quick reference to additional evidence requirements
- Guide to using the online Toolkit
- Frequently asked questions



The NHS Information Governance requirements are reviewed and updated annually. There have been a number of changes to the NHS Pharmacy Information Governance Requirements in 2010/11. These are outlined in the latest version of the online Information Governance Toolkit, version 8.

Deletions

Requirement 118 (Completion of IGSoC) has been removed as a requirement.

Additions / Business Continuity

The only major addition to the requirements in 2010/11 is, as previously communicated, the business continuity requirement (requirement 319). PSNC is in discussion with the Department of Health on this requirement including the detailed scope of business continuity plans and the timescale for completing business continuity planning.

It is important that pharmacies have well-prepared and robust business continuity plans to help overcome any unexpected event that impacts on the day to day operation of the pharmacy. In developing plans, contractors will need to undertake local communication and engagement and this will take time. It is important that pharmacies have a reasonable timescale to complete this work. As soon as more information is available on PSNC's discussions with the Department of Health on this requirement, it will be posted on the PSNC website (www.psn.org.uk).

The PSNC are finalising a template business continuity impact document and plan, it is currently under review in light of learning from recent events including the adverse weather conditions in late 2010.

Merged Requirements

Requirements 208 (mapping and risk assessing information flows) and requirement 308 (exchange of digital information) have been merged to form one requirement. There was overlap between the two original requirements. Requirement 208 was predominantly focussed on safe havens and the manual transfer of information and requirement 308 was focussed on digital transfer. The new merged requirement is 'all transfers of hardcopy and digital personal and

sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers'. The reference number for the new requirement is '8-322'. The evidence required by pharmacies remains the same.

Refinement of Requirements

Numerous minor changes have been made to the requirements and in some cases there is a need for pharmacies to obtain additional evidence to that published in the January 2010 Pharmacy Contractor workbook. A cross-reference of the version 7 (2009/10) and 8 (2010/11) requirements with details of the additional evidence required can be found on pages 4-8.

Nationally developed supporting resources including the template staff confidentiality code of conduct, asset register and audit checklist have been updated in line with the refinement to the requirements and a large print version of the patient information leaflet has been developed. These can be found on the PSNC website (www.psn.org.uk/IG).

Numbering of Requirements

From version 8 of the Toolkit (2010/11), the reference number of each requirement will be prefixed with the online toolkit version number, i.e. requirement 114 is requirement 8-114 for 2010/11 and for version 9 in 2011/12, it will be 9-114. Also a number of the requirements have been re-numbered, for example, requirement 119 has been re-numbered requirement 8-304.

The Online Toolkit

There have been some significant changes to the way the online toolkit looks and operates since pharmacy contractors last submitted an assessment in early 2010. The basic structure of the assessment remains the same. The website has been designed by DH to be user-friendly and intuitive. A quick reference guide to the Toolkit can be found on page 9 and if needed, a detailed user guide to carrying out an IG Assessment can be found on the PSNC website (www.psn.org.uk/IG).

For each requirement, it is necessary to make some comments to support the declared score, this could be by making some comments in the general comments

box or ticking the relevant evidence obtained boxes. There are optional fields to record where evidence is located including the option to upload evidence and an option to record details linked to a specific piece of evidence – however it is not mandatory to complete these fields.

Transparency of Scores

Following a number of FOI requests, the Department of Health has published the overall scores for all organisations that have made a Toolkit assessment, this includes the baseline assessments that were submitted by community pharmacies last year. It is expected that the Department of Health will, in due course, publish the overall scores for individual pharmacies that make a return via version 8 of the online Toolkit. This information can be accessed via the Information Governance Toolkit website (www.igt.connectingforhealth.nhs.uk/).

Timescales

By 31 March 2011 community pharmacies will be expected to attain Level 2 against each of the pharmacy information governance requirements. However PSNC is still in discussion with the Department of Health on the timescale for completing business continuity planning (requirement 8-319).

Funding

As part of the 2009/10 community pharmacy contractual framework funding settlement, the DH and PSNC agreed an allocation of £23 million of funding to support the implementation of the Information Governance requirements. This equates to over £2000 for the average pharmacy contractor. This was paid out through the general funding arrangements rather than via a specific fee. PSNC is currently in discussion with the Department of Health to finalise the funding allocation for business continuity planning. To date £12m has been allowed. As with the Information Governance funding, this was paid out through the general funding arrangements rather than via a specific fee.

There are also ongoing costs, in maintaining compliance with the requirements, making annual Information Governance returns via the Toolkit and

The chart below is a quick reference guide to the key actions required to ensure Level 2 compliance with the NHS IG requirements. Actions shaded in light green have either been added or refined since the January 2010 Pharmacy Contractor Workbook was published. A summary of the 2010/11 changes can be found on pages 4-8. Full details of the requirements can be found in the online Information Governance Toolkit. Templates to support providing evidence of compliance with each requirement can be downloaded from the PSNC website (www.psn.org.uk/ig).

- Minimum Actions by 31st March 2011**
- Appoint IG Lead(s) (Requirement 8-114)
 - Take time to understand the requirements (e.g. read the NHS IG: Pharmacy Contractor Workbook (January 2010) and this update booklet)
 - Gather evidence that responsibility for certain tasks has been assigned to someone where required (8-117 (training), 8-209 (international data transfers), 8-304 (smartcards), 8-316 (asset register), 8-320 (incident management), 8-321 (administering access rights))
 - Develop an IG policy (Requirement 8-115 / Template 1)
 - Ensure there are appropriate contractual clauses in staff and third party contracts (Requirement 8-116 / Template 2)
 - Ensure staff are sufficiently trained in IG (Requirement 8-117 / Booklet "Introduction to Information Governance for Pharmacy Staff")
 - Identify any overseas data transfers and put in place mitigating controls (Requirement 8-209)
 - Create a patient information leaflet on how data is handled by the pharmacy and consider how to communicate this information where there are special needs (Requirement 8-213 / Template 5 / Large print template leaflet available as Template 5B)
 - Develop a staff confidentiality code of conduct (Requirement 8-214 / Template 3)
 - Ensure there is a plan in place to monitor and enforce RA01 Smartcard Terms (Requirement 8-304 / Template 16/NB Only applies to EPS Release 2 cards)
 - Create an information asset register (Requirement 8-316 / Template 6)
 - Risk assess physical security (Requirement 8-317 / Template 7)
 - Resources to support mobile computing (Requirement 8-318 / Template 8-10)
 - Develop an incident management procedure (Requirement 320 / Template 11)
 - Put in place an IG incident log (Requirement 8-320 / Template 12)
 - Develop an access control procedure (Requirements 8-321 / Template 15)
 - Map, risk assess and put in place mitigating controls on data transfers (Requirement 8-322 / Appendix 7 of the January 2010 Pharmacy Contractor Workbook)
 - Develop one or more procedures that cover data transfer, safe havens and seeking patient consent (Requirements 8-212 and 8-322 / Template 4)
 - Ensure policies, procedures and guidance materials are signed off by an appropriately senior staff member (Various)
 - Ensure staff have been informed, where relevant (Various / Template 14)
 - Put in place a system to monitor staff compliance with key requirements (Various / Template 13)
 - Complete Online Toolkit by 31st March 2011 and generate work plan

NB: There will be a need to develop a business continuity impact document and plan (requirement 8-319). PSNC is in discussion with the Department for Health on both the scope of this work and timescales for completion. Once agreed, more information will be available on the PSNC website.

implementing changes made to the requirements by the NHS. As part of the funding arrangements for the national contractual framework. Annual adjustments are made to pharmacy funding to reflect costs necessitated by

significant additional regulatory burdens on contractors. Regulatory burdens are assessed on a retrospective basis. PSNC will be negotiating with the Department of Health on funding to cover ongoing costs.

Going forward

Whilst there may be minor changes to the requirements in 2011-12, early indications are that there will not be significant changes to the requirements within the next year.

The table below provides a cross-reference of the version 7 and 8 requirements with details of the additional evidence required. Changes that relate to Level 1 and Level 2 requirements are highlighted in green. By 31 March 2011, all community pharmacies will be expected to attain Level 2 compliance against each of the pharmacy information governance requirements. Whilst some pharmacies may achieve Level 3 compliance with some of the requirements, this is not mandatory. Templates and other resource material to support providing evidence of compliance with the requirements can be found online at www.psn.org.uk/IG.

Version 7 IGT Ref.	Version 8 IGT Ref.	Version 8 Requirement Statement	Changes to the requirements as outlined in the NHS Information Governance Pharmacy Contractor Workbook (January 2010)	Evidence Suggestions
114	8-114	Responsibility for Information Governance has been assigned to an appropriate member or members of staff	Addition: As a Level 2 requirement, evidence is required that a contractor representative has signed-off the workplan/improvement plan.	Note the name of the contractor representative in the pharmacy IG file.
			Addition: As a Level 3 requirement, evidence is required of progress against the improvement plan being monitored in-year and reports made to senior staff.	Meeting notes, emails confirming tasks have been undertaken or notes in the pharmacy IG file tracking progress.
115	8-115	There is an Information Governance Policy that addresses the overall requirements of Information Governance	Addition: As a Level 3 requirement, contractors need to demonstrate that staff understanding of the IG policy and it's relevance to the way they work is being assessed, for example through compliance spot checks.	The template 'IG Internal Audit Checklist' (IG template 13) has been amended to include a spot check question that would support meeting this requirement.
116	8-116	All contracts (staff, contractor and third party) contain clauses that clearly identify Information Governance responsibilities	Addition: There is now a Level 1 requirement that a contractor representative has signed off the confidentiality clauses used in contracts.	Note in the pharmacy IG file, the date and the name of the contractor representative that signed off the clauses.
			Addition: As a Level 1 requirement, if all staff and third party contractors don't already have appropriate confidentiality clauses in their contracts, there is a need to document an action plan on updating contracts.	The action plan could be a note in the pharmacy IG file confirming targets for getting this done.
			Change and addition: Previously there was a Level 2 requirement to list all third party contractors with access to personal information. This requirement has been moved to Level 1 and extended to include a list of all staff, contractors and third parties with access to personal information.	A written note in the pharmacy IG file or a reference to lists held in another part of the business e.g. referencing a list of employees held by the payroll department to prevent duplicating staff lists.
			Addition: There is now a Level 3 requirement that staff, contractors and other third parties' compliance with IG responsibilities is tested through spot checks and routine monitoring.	Undertaking internal audits using a checklist such as the template IG internal audit checklist (template 13) is sufficient to meet this requirement.
117	8-117	All staff members are provided with appropriate training on Information Governance requirements	Addition: There is now a Level 1 requirement to assign responsibility for arranging appropriate IG training for all staff to a named individual. This could be the IG Lead, a training lead or another member of staff.	Written assignment of responsibility (e.g. note in the pharmacy IG file).
			Change: A Level 1 requirement is that all new starters should receive basic IG training.	Signature list confirming training has been received (e.g. the staff member has read the IG training booklet for pharmacy staff).
			Change: Basic IG awareness training must now be provided to all staff to achieve Level 2 rather than simply to key staff.	Staff signature list (e.g. template 14).
			Addition: A new Level 2 requirement is that the training needs of staff is assessed to ensure that the basic training provided is sufficient and staff in key roles are provided with additional training when required.	Staff understanding could be assessed by using routine in-house audits, for example using an audit checklist (e.g. template 13 – updated). Where problems with staff understanding are identified, further training could be arranged.

Version 7 IGT Ref.	Version 8 IGT Ref.	Version 8 Requirement Statement	Changes to the requirements as outlined in the NHS Information Governance Pharmacy Contractor Workbook (January 2010)	Evidence Suggestions
117 cont.	8-117 cont.		Additions: New Level 3 requirements include testing staff knowledge, for example through internal audits and providing evidence that remedial training is provided where needed. There is also a Level 3 requirement that the training materials are reviewed annually to ensure they meet the needs of the organisation.	An audit checklist (e.g. template 13) could be used to check staff knowledge and identify problems. Notes could be made in the pharmacy IG file that additional training was given to staff where needed and to confirm the review of training materials.
118	N/A	N/A	Deleted Requirement (Has the pharmacy implemented robust IG arrangements to ensure the NHS CFH IG Statement of Compliance (IGSoC) is satisfied?)	
119	8-304	N/A	Requirement re-numbered.	
208	N/A	N/A	Merged with 308 to form 8-322.	
209	8-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Addition: There is now a Level 1 requirement to assign responsibility for reviewing information flows to identify overseas transfers. The IG Lead or another member of staff could take on this responsibility. Change: Where there are flows of data outside of the UK, it is now a Level 2 requirement to ensure that arrangements are in place to ensure compliance with the Data Protection Act and DH guidance. This change was made to ensure the NHS IG requirements were in line with the legal requirements in this area.	Written assignment of responsibility (e.g. note in the pharmacy IG file). No further evidence is required.
			Addition: It is a Level 3 requirement to review arrangements annually to ensure continued compliance with the law.	Make a note in the pharmacy IG file to confirm annual review.
212	8-212	Consent is appropriately sought before personal information is used in ways that do not directly contribute to the delivery of care services and objections to the disclosure of confidential personal information are appropriately respected	Addition: It is now a Level 2 requirement to provide evidence that guidelines on seeking patient consent are accessible to pharmacy staff.	Note the location of the guidelines in the pharmacy IG file.
			Addition: It is now a Level 3 requirement to use a patient satisfaction survey to check that patients understand their consent choices and feel that their wishes are respected.	A sample question that could be used can be found on the PSNC Website (www.psn.org.uk/IG).
			Addition: It is now a Level 3 requirement to annually review guidance for staff on seeking patient consent.	Make a note in the pharmacy IG file to confirm annual review.
213	8-213	There is 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 rights to see and obtain copies of their records	Addition: It is now a Level 1 requirement to provide evidence to confirm that the patient leaflet has been signed-off by a contractor representative.	Make a note of the contractor representative in the pharmacy IG file.
			Change: The need to ensure that staff are briefed on patient communication materials has been moved from Level 3 to Level 2.	A staff signature list could be used as evidence of this (e.g. template 14).
			Addition: There is a new Level 2 requirement that where necessary, communications materials are provided in different formats or by different routes to meet the need of patients with special or different needs.	A template large print patient information leaflet has been developed to support meeting this requirement (template 5B). Make a note in the pharmacy IG file of how special needs are met. NHS Direct provide an interpreter service to support communicating with patients who do not speak English (www.nhsdirect.nhs.uk/About/CallingNHSDirect/InterpreterService).
			Addition: There is a new Level 3 requirement that all written communications with patients include advice on the way that patient	Where a pharmacy contractor is writing to a patient or member of the public in relation to NHS services, and the communication includes or requests any personal or sensitive information, *where practical,

Version 7 IGT Ref.	Version 8 IGT Ref.	Version 8 Requirement Statement	Changes to the requirements as outlined in the NHS Information Governance Pharmacy Contractor Workbook (January 2010)	Evidence Suggestions
213 cont.	8-213 cont.		information is used and shared, and how patients can gain access to their own records. Details of which staff member to approach for further assistance is also made available.	<p>the communication should include advice on the way that patient information is used and shared, how patients can gain access to their own records and details of which staff member to approach for further assistance.</p> <p>This requirement could be met in a number of ways including enclosing a copy of the pharmacy information leaflet on safeguarding information or including a brief cross-reference to where the patient can source more information in the text of the letter (for example, 'For more information on our data protection policies and practices, please see a copy of our information leaflet, "How we look after and safeguard information about you").</p> <p>*In limited circumstances it may not be practical to provide a copy of the leaflet or include a cross reference in every individual communication (e.g. text messaging due to limits on the number of characters that can be used). In these circumstances, one possibility could be advising the patient or member of the public on the way that patient information is used and shared when initially collecting consent to communicate with the patient in this way.</p>
201 (small-org)	8-214	There is a confidentiality code of conduct that provides staff with clear guidance on the disclosure of personal information	Addition: It is now a Level 3 requirement to use a patient satisfaction survey to check that patients feel that their confidentiality is respected and that they trust the organisation to hold information securely.	A sample question that could be used can be found on the PSNC website (www.psn.org.uk/IG).
119	8-304	Monitoring and enforcement processes are in place to ensure NHS national application smartcard users comply with the terms and conditions of use	<p>Addition: There is now a Level 1 requirement to assign responsibility for developing a plan to monitor and enforce user compliance with regard to Smartcard usage. This could be the IG Lead or another member of staff.</p> <p>Change: There is a change to the Level 1 requirement to document a plan for monitoring compliance with the RA01 Terms and Conditions. This requirement has been extended to include informing users of their responsibilities regarding smartcard usage.</p> <p>Addition: It is now a Level 1 requirement to provide evidence to confirm that the plan and associated procedures to inform users of their responsibilities regarding smartcard usage and for monitoring compliance have been signed-off by a contractor representative.</p> <p>Addition: It is now a Level 2 requirement that procedures for dealing with breaches in smartcard usage are accessible to users.</p> <p>Addition: A new Level 3 requirement is to use awareness raising measures to ensure users remain compliant with the terms and conditions of smartcard usage.</p> <p>Addition: A new Level 3 requirement is to regularly review enforcement and compliance arrangements to ensure they continue to be effective.</p>	<p>Written assignment of responsibility (e.g. note in the pharmacy IG file).</p> <p>Evidence could be a note in the pharmacy IG file on how compliance checks will be undertaken and how the terms and conditions will be communicated to staff e.g. staff given the RA01 terms and Conditions and asked to sign a signature list. A new template has been developed to support meeting this requirement (template 16: ensuring staff compliance with RA01 terms).</p> <p>The name of the contractor representative could be noted in the pharmacy IG file.</p> <p>Evidence could be noting the location of the procedures. The staff confidentiality code (e.g. template 3) could be used as the document which details sanctions for breaches in the terms and conditions. The template confidentiality code has been amended to include a reference linked to compliance with the NHS terms and conditions for smartcards.</p> <p>Evidence of this could be a note of the method used to raise awareness e.g. a reminder to staff.</p> <p>Make a note in the pharmacy IG file to confirm annual review.</p>

Version 7 IGT Ref.	Version 8 IGT Ref.	Version 8 Requirement Statement	Changes to the requirements as outlined in the NHS Information Governance Pharmacy Contractor Workbook (January 2010)	Evidence Suggestions
316	8-316	There is an Information Asset Register that includes all key information, software, hardware and services	Change: The scope of the asset register has changed to include maintaining information on services (e.g. information on the broadband connectivity provider and telecoms provider) as well as information, software and physical assets. Note whilst it is important that the pharmacy has access to a list of their telecoms and IT service providers for business continuity reasons, there could be a cross-reference from the asset register to this list of services if it is maintained separately rather than duplicating this information. As information asset registers are likely to contain commercially sensitive information, there is no requirement for the details of the register to be shared with PCTs.	The template asset register (template 6) has been updated to include services.
317	8-317	Unauthorised access to the premises, equipment, records and other assets is prevented	Addition: A new Level 2 requirement is that staff members, including new staff, have been informed about new security measures put in place (where applicable) and the process for reporting unauthorised access.	Evidence of this could be a note in the pharmacy IG file indicating how staff have been informed e.g. through an email, a discussion with staff etc.
			Addition: A new Level 3 requirement is undertaking compliance spot checks to confirm security procedures are being followed by staff. Note there is no requirement to share information on the pharmacies security procedures with PCT staff.	Evidence of this could be a checklist used to undertake in-house audits. A number of questions have been added to the template audit checklist (template 13) to meet this requirement.
318	8-318	The use of mobile computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access	Addition: A new Level 2 requirement is that access to internal IT systems is controlled and there are robust authentication procedures in place for all staff having remote access to systems. This means that if a staff member is able to remotely access the pharmacy IT system (e.g. by dialling in from home, from a patient's home, or from another of the organisation's sites), this must only be allowed if there is a process of strong authentication through token or biometric mechanisms e.g. an equivalent to the NHS Smartcard.	Evidence to meet this requirement would be a declaration of the mechanism used to control access e.g. a note in the pharmacy IG file.
			Addition: A new Level 2 requirement is comprehensive guidance for staff on the correct operation of mobile computing equipment and the prevention of unauthorised access. The existing Template 8 (Mobile Computing Guidelines) is sufficient to meet this requirement.	No further evidence is required.
			Addition: A new Level 3 requirement is that audits are carried out to ensure that equipment is appropriately allocated. The original version of the Template Audit Checklist (Template 13) includes a question to comply with this requirement.	No further evidence is required.
			Addition: A new Level 3 requirement is to review annually, the robustness of security and access controls to take account of any changes made to the technical access controls in systems.	Make a note in the pharmacy IG file to confirm annual review.

Version 7 IGT Ref.	Version 8 IGT Ref.	Version 8 Requirement Statement	Changes to the requirements as outlined in the NHS Information Governance Pharmacy Contractor Workbook (January 2010)	Evidence Suggestions
319	8-319	There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions	As previously communicated, this requirement has been added for 2010/11. There will be a need to develop a business continuity impact document and plan. PSNC is in discussion with the Department for Health on both the scope of this work and timescales for completion. Once agreed, more information will be available on the PSNC website.	PSNC is developing a range of support material including a template business continuity impact document (template 17) and a template business continuity plan (template 18). As soon as these resources are finalised, they will be published on the PSNC website (www.psn.org.uk/IG).
320	8-320	There are documented incident management and reporting procedures	<p>Addition: A new Level 3 requirement is that compliance checks are undertaken to ensure staff understand and are complying with incident management and reporting procedures.</p> <p>Addition: A new Level 3 requirement is that information incidents and near-misses are appropriately discussed with staff.</p>	<p>The template audit checklist (template 13) has been updated with questions to ensure compliance with this requirement.</p> <p>Evidence of this could be a note in the pharmacy IG file with some examples of discussions that have taken place.</p>
305 (small-org)	8-321	There are appropriate procedures in place to manage access to computer-based information systems	<p>Addition: There is now a Level 1 requirement to assign responsibility for allocating and removing access rights to the system. This could be the IG Lead or another member of staff.</p> <p>Addition: There is a new Level 2 requirement that access to information assets is only possible for individuals who have been duly authorised.</p> <p>Addition: A new Level 3 requirement is that access requirements are routinely reviewed to ensure that user access privileges remain appropriate, and where access is no longer required, it is disabled or revoked.</p> <p>Addition: A new Level 3 requirement is that the access control procedures are reviewed annually to ensure they take account of any changes made to the technical access controls in systems.</p>	<p>Written assignment of responsibility (e.g. note in the pharmacy IG file or in the access control procedures).</p> <p>Having access control procedures is sufficient evidence for this requirement (template 15). No additional evidence needed.</p> <p>This could be evidenced through the use of in-house audits. The audit template (template 13) has been updated to meet this requirement.</p> <p>Make a note in the pharmacy IG file to confirm annual review.</p>
308+208 merged (small-org)	8-322	All transfers of hardcopy and digital personal and sensitive information have been identified, mapped and risk assessed. Technical and organizational measures adequately secure these transfers	<p><i>This requirement has been formed from the merger of version 7 requirements 208 and 308.</i></p> <p>Addition: An additional Level 3 requirement is that flows of personal and sensitive information are reviewed annually and records are updated to reflect any changes in flow methods, locations or data items.</p>	Make a note in the pharmacy IG file to confirm annual review.

The Toolkit can be accessed at: www.igt.connectingforhealth.nhs.uk

Logging in to the Toolkit

A pharmacy must be registered to complete the online IG assessment. If you have previously registered, login using your organisation code (ODS Code), user name and password. The ODS code is commonly referred to as the 'F code' and can be found at the top of the 'Schedule of Payments' received from NHS Prescription Services. If the nominated individual has forgotten their password to login to the IG Toolkit, the password can be easily recovered by clicking on the "Forgotten user details?" link under the "Registered Users" heading on the site. The "forgotten user details" page allows the nominated individual to recover the lost password by entering the email address that was used to register the pharmacy.

If there has been a *change of ownership* since the last Toolkit assessment was submitted and the pharmacy ODS code has stayed the same, the new owner should contact the DH Informatics Helpdesk (0113 394 6540). The account of the previous owner can be locked and the new owner registered against that ODS code. Likewise, if the *nominated user of the toolkit has left the pharmacy* since the last Toolkit submission, contact the DH Informatics Helpdesk so that another user can be registered to use the toolkit.

If your pharmacy has *not previously registered* for access to the site, select the "Register" button in the new users section of the Toolkit homepage. Only one registration can be made per pharmacy. Ensure the email address is correct as this is how NHS CFH will contact the nominated individual with information about the IG Toolkit.

Completing the Assessment

There have been some significant changes to the way the online toolkit looks and operates since pharmacy contractors last submitted an assessment in early 2010. The basic structure of the assessment remains the same.

Key points to be aware of:

- If a version 7 assessment had been

started in early 2010 but wasn't finished or the 'submit' button wasn't clicked, it will be necessary to either complete the version 7 assessment or re-set the assessment to allow the Version 8 assessment to be completed.

- For each requirement, under "Attainment Levels", there is now a built-in checklist of criteria for each attainment level. When completing your assessment, you tick off the *criteria* that you have achieved and the system automatically determines your attainment level. The criteria are cumulative – in order to achieve Level 2 you must first achieve all criteria for Level 1.
- It is important to make some comments to support your score, this could be by making some comments in the comments box or ticking the relevant evidence obtained boxes. There are optional fields to record where evidence is located and record details linked to a specific piece of evidence – but it is not mandatory to complete these fields. There is no requirement to upload evidence.
- Finally, there is a need to enter a 'target level' and a 'target date'. There is no requirement for pharmacies to achieve Level 3 compliance so the target level could be continuing to meet Level 2. The target date could be the 31st March 2012.

Submitting the assessment

Once you are satisfied that the scores recorded accurately reflect the pharmacy's level of compliance with the IG requirements, you should select the "Assessments" option (on the left hand side) and then click the "Submit" button.

When the assessment has been submitted, the Toolkit will confirm this on-screen by showing the status as

Req No	Req Title	Criteria	Attainment	Comments	Level
Version 8 (2010-2011) Assessment					
Requirement 1: Access to Data Management					
R101	Supports data management, including data transfer, data backup and data recovery.	Not assessed	Not assessed		Level 1
R102	The Toolkit is available on a secure web site that is accessible to all staff.	Not assessed	Not assessed		Level 1
R103	All records held on the Toolkit are protected by a secure password.	Not assessed	Not assessed		Level 1
R104	All data held on the Toolkit is protected by a secure password.	Not assessed	Not assessed		Level 1
Requirement 2: Data Protection					
R201	All data held on the Toolkit is protected by a secure password.	Not assessed	Not assessed		Level 1
R202	Access to data held on the Toolkit is restricted to authorised staff only.	Not assessed	Not assessed		Level 1
R203	All data held on the Toolkit is protected by a secure password.	Not assessed	Not assessed		Level 1
R204	All data held on the Toolkit is protected by a secure password.	Not assessed	Not assessed		Level 1
Requirement 3: Security, Network					
R301	Access to data held on the Toolkit is restricted to authorised staff only.	Not assessed	Not assessed		Level 1

submitted and an email will be sent to confirm this to the email address associated with the online Toolkit account.

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.

Contractors with more than one pharmacy

Currently 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.

Help

If needed, a more in-depth, step-by-step user guide to making an online Toolkit submission can be found on the PSNC website (www.psn.org.uk/IG).

Support in registering and using the toolkit is available from the DH Informatics Helpdesk at pharmacy.assurance@nhs.net or telephone 0113 394 6540.

Support on the Information Governance requirements is available from a range of sources including the PSNC Information Team (01296 432823 or email info@psnc.org.uk) and the DH Informatics Helpdesk (0113 394 6540 or email pharmacy.assurance@nhs.net). Frequently asked questions include:

1. Can a PCT take action against a pharmacy contractor who does not achieve Level 2 compliance by the 31st March 2011?

Compliance with the NHS Information Governance Requirements is not yet a specific contractual requirement; however there are provisions in the Terms of Service relating to pharmacy compliance with the Data Protection Act 1995 and the NHS Code of Practice on Confidentiality.

The Information Commissioner's Office (ICO) enforces and oversees the Data Protection Act. In April 2010, the ICO was given new powers to fine organisations up to £500,000 as a penalty for serious breaches of the Data Protection Act. When serving monetary penalties, the Information Commissioner will carefully consider the circumstances, including the seriousness of the data breach; the likelihood of substantial damage and distress to individuals; whether the breach was deliberate or negligent and what reasonable steps the organisation has taken to prevent breaches. The ICO has published guidance on what they consider to be 'reasonable steps'. This includes things like putting in place appropriate policies and procedures, undertaking risk assessments and putting in place appropriate mitigation to safeguard data and having

good governance/audit arrangements to prevent contraventions of the Data Protection Act. These are all actions that the NHS requires evidence of through the NHS Information Governance Toolkit.

A PCT may investigate a pharmacy that has not completed an annual return via the Information Governance Toolkit to satisfy itself that the pharmacy is meeting the Terms of Service requirements.

The expectation is that compliance with the NHS requirements and annual completion of the Information Governance Toolkit will become specific contractual requirements, in due course.

The focus for PCTs should be on supporting pharmacy contractors with implementation of these requirements. Contractors requiring support or who are concerned about their ability to provide evidence to demonstrate compliance with any of the requirements should discuss this with the PCT.

2. When will more information be available on the business continuity requirement (requirement 8-319)?

PSNC is currently actively discussing the detailed scope and timescale for this requirement with the Department of Health. It is important that pharmacies have well-prepared and robust business continuity

plans to help overcome any unexpected event that impacts on the day to day operation of the pharmacy. In developing plans, contractors will need to undertake local communication and engagement and this will take time. It is important that pharmacies have a reasonable timescale to complete this work. As soon as more information is available on PSNC's discussions with the Department of Health on this requirement, it will be posted on the PSNC website (www.psn.org.uk).

3. I submitted a baseline assessment using Version 7 of the Toolkit last year. Is there any way to copy across the information I filled in last year?

No, unfortunately it is not possible to copy across previous scores. All information needs to be entered afresh.

4. A number of the requirements ask for a policy or procedure to be signed off by a contractor representative. Who is the 'contractor representative'?

A "contractor representative" could be anyone who has been authorised to represent a contractor for a particular purpose. This has not been defined further as different pharmacies will have different business models, for example it could be a director of the company, a board of directors, or someone appointed within

a company to undertake the role. An IG Lead could be given the authority to sign off policies linked to IG. It is also possible for the person responsible for developing the policy to be the same as the person that has the authority to sign off the policy (e.g. if the owner of an independent pharmacy is preparing the policy them self). The representative doesn't need to be a pharmacist.

5. On the Information Governance Toolkit, there are fields linked to each requirement to record the location of evidence or to upload evidence. Do I need to complete these fields?

No. It is important to make some comments to support your score, this could be by making some comments in the comments box or ticking the relevant evidence obtained boxes but it is not mandatory to complete the optional fields to record where each piece of evidence is located or to upload evidence such as policies and procedures.

Note some evidence will include commercially sensitive information and would therefore be inappropriate to upload.

6. I currently don't use any mobile computing systems in my pharmacy. There is no 'Not Relevant' option on the Toolkit for requirement 8-318 (mobile computing), how should I record this requirement?

If the pharmacy does not use any mobile computing devices i.e. there are no laptops and PDAs, nor any

portable device used to hold or transfer personal information (e.g. USB sticks and CDs/DVDs), 'Level 3' can be recorded but the pharmacy should insert a comment in the text field that states the requirement is not applicable, and that their policy is that they have no mobile computing devices. For example: "Requirement not applicable, this pharmacy does not use removable or portable computing equipment including CDs/DVDs and USB sticks." The pharmacy should ensure that staff do not use mobile computing devices in their role.

7. I am currently using EPS Release 1 and no staff in my pharmacy have EPS Release 2 Smartcards (RA01 Terms and Conditions). Do I need to comply with requirement 8-304 (Smartcards)?

No. This requirement relates to monitoring and enforcement processes to ensure staff compliance with the RA01 terms and conditions that apply to EPS Release 2 smartcards. This requirement can be marked 'not relevant' if no staff in the pharmacy have EPS Release 2 cards.

Following requests from contractors who do need to comply with this requirement,

PSNC has developed a simple 'ensuring staff compliance with RA01 terms' template SOP. This can be downloaded from the PSNC website (www.psn.org.uk/IG).

8. I currently maintain a comprehensive list of the hardware and software I own for insurance purposes. Do I need to also maintain this information in a separate Information Asset Register?

There are no mandatory requirements for how the information asset register should be structured but it should include information on information stored (e.g. patient databases), hardware,

software and services (e.g. broadband connectivity). Where the pharmacy maintains information on software, hardware or services in a separate asset register for accounting, insurance or business continuity purposes, an option is to do a cross reference from the relevant sections in the information asset register to the relevant register or location that this information is stored to prevent duplicating effort.

More frequently asked questions on the requirements can be found on the PSNC website (www.psn.org.uk/IG).

Information Governance Top Tips

1. Start now and don't panic - it will take time to complete but it is achievable.
2. Read the PSNC guidance and take time to plan your approach to completing the requirements.
3. Lighten the load: Get your team involved – delegate tasks to capable senior staff. The IG Lead doesn't have to do all of the work. The IG Lead doesn't need to be a pharmacist.
4. It may be easier to set aside some time to concentrate on completing this work, rather than doing in small chunks in between other jobs. Once you have cracked the process, it is gets quicker to complete.
5. Don't reinvent the wheel. There are templates available to meet each of the requirements. Adapt these to meet your needs rather than starting from scratch.
6. If in doubt, ask for help. Many PCT IG leads are happy to answer questions

directly. Support is also available from other organisations including PSNC, Avicenna and Numark.

7. Run a communication/training session with all staff to position IG, and then send the IG folder on a 'round robin' for necessary reading and signing.
8. When completing the online Toolkit, once you have entered information on all of the requirements, make sure you click the 'submit' button. On-screen the status will change to 'submitted' once you have done this and a confirmation email will be sent to the email address associated with the account.
9. Be organised – have everything in one place or folder. PCTs are likely to want to see evidence during monitoring visits.
10. Put the review dates into your diary NOW – that way they don't get forgotten

11. Keep an easily accessible record of your log-on details for the online Toolkit – it will be very handy for future years.

12. Finally, instead of seeing IG as another burdensome requirement, take the opportunity to use it to identify and improve areas of your business – make it work for YOU!

Thanks to Avicenna, Numark and all of the contractors who submitted tips.



Organisation	Contact Information	Type of Support
DH Informatics Helpdesk	Email: pharmacy.assurance@nhs.net Tel: 0113 394 6540 Web: www.igt.connectingforhealth.nhs.uk	General guidance on the requirements and technical support in using the IG Toolkit.
PSNC Information Team	Email: info@psnc.org.uk Tel: 01296 432823 (Option 1) Web: www.psn.org.uk/IG	General guidance on the requirements.
Information Commissioner's Office	Tel: 08456 30 60 60 Web: www.ico.gov.uk	Guidance on the Data Protection Act.
PCT	IG Lead	Additional support in working through some of the requirements may be available locally.
RPS support (The Royal Pharmaceutical Society)	Tel: 0845 257 2570 Email: support@rpharms.com	General guidance for RPS members on issues related to confidentiality and consent.

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**

