IG Requirement Assurance Tool (IGT)

Requirements Booklet

Commercial Third Party

Version 11

Req No	Description	Page
Information Governance Management		
11-114	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff	3
11-115	There is an information governance policy that addresses the overall requirements of information governance	11
11-116	All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities	19
11-117	All staff members are provided with appropriate training on information governance requirements	31
Confidentiality and Data Protection Assurance		
11-202	Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected	39
11-206	There are appropriate confidentiality audit procedures to monitor access to confidential personal information	49
11-209	All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	57
11-210	All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements	65
11-211	All transfers of personal and sensitive information are conducted in a secure and confidential manner	79
Information Security Assurance		
11-305	Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems	89
11-313	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	105
11-314	Policy and procedures ensure that mobile computing and teleworking are secure	113
11-316	There is an information asset register that includes all key information, software, hardware and services	123
11-317	Unauthorised access to the premises, equipment, records and other assets is prevented	129
11-319	There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions	137
11-320	There are documented incident management and reporting procedures	147
11-323	All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	159

Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff	Requirement No:	11-114
	Initiative:	Information Governance Management
	Organisation Type:	Commercial Third Party
	Version:	11.1

Requirement Description

It is important that that there is a consistent approach to information handling within the organisation which is in line with the law, central policy, contractual terms and conditions and best practice guidance. This requires one or more members of staff to be assigned clear responsibility for driving any required improvements.

Responsibility for Information Governance

Introduction

1. This requires that named individuals take responsibility for co-ordinating, publicising and monitoring standards of information handling within the organisation and for developing and implementing an IG improvement plan (also known as implementation or work plan). The Information Governance Lead(s) also need(s) to ensure that IG Toolkit assessments are submitted as required.

Appointing an IG Lead

2. The senior management should consider the responsibilities of an IG 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 organisations with multiple premises there may be a need to appoint an overall lead with other staff supporting at the premises level. Those appointed should have sufficient seniority and authority to ensure that any necessary changes in information handling within the organisation can be implemented and enforced.
3. Example implementation models include:
    a. If a contractor is supported by a substantial head office function, a member of head office staff may be appointed to co-ordinate information governance across the organisation however there will still be a need for a local IG lead to co-ordinate local IG activities such as developing an improvement plan (see **paragraph 11**) relevant to the local circumstances and supporting a monitoring visit from the *commissioning organisation*.
    b. If a contractor runs an individual business the IG lead would typically be a senior permanent member of the staff.
4. Ensuring confidentiality is already a key part of the clinical governance requirements in most contractual frameworks. IG responsibilities can be combined with other

similar responsibilities, e.g where there is a contractual framework requirement for an organisation to have an identifiable clinical governance lead, this individual might also act as the IG Lead.

5. There should be written assignment of IG Lead responsibility. This could be through adding this to staff job descriptions or simply a written note explaining the position.

What Training and Support does the IG Lead Require?

6. An IG Lead needs to be sufficiently trained to undertake their key responsibilities. Training should cover data protection, security and confidentiality and Freedom of Information requirements. Training can be undertaken through the on-line NHS Information Governance Training Tool.

7. The IG Training Tool comprises a structured e-learning programme with Introductory, Foundation and Practitioner level modules covering all aspects of IG. The organisation needs to be registered in the Tool before users can set up an account, and ideally an organisation administrator should be nominated and given the appropriate permissions to monitor staff training. This can all be arranged by logging a request with the IG Training Tool helpdesk complete the Contact Us section providing the organisation name, corporate email domain (if one exists) and ODS code, (also known as the practice code, the national code, or the pharmacy F code found on the submission document used to send prescriptions to NHS Prescription Services).

8. Once the organisation is registered, other members of staff will be able to register on the Tool. As part of the user registration process, staff will be asked for their organisation's ODS code, so it is important to ensure staff know what the code is before they attempt to register. If no corporate email domain exists, staff can still register by selecting "no" when asked if they have a work email and following the steps to create an onscreen account.

9. The IG Lead should also have access to sufficient support to do their job and if s/he is not a health or care professional (eg pharmacist, optician, ophthalmologist, GP, dentist, etc) or a senior manager, they will need access to such a person for support with queries.

Responsibilities of an Information Governance lead

10. The IG lead is not required to carry out all the work necessary to meet the NHS IG requirements, but should be able to supervise and direct the work of others where necessary. Table 1 provides a summary of the key responsibilities of the Information Governance lead.

Table 1: Key responsibilities of an Information Governance lead
• ensure there is an up to date IG policy in place; • ensure that the organisation's approach to information handling is communicated to all staff and made available to the public; • coordinate the activities of staff given data protection, confidentiality and Freedom of Information responsibilities; • monitor the organisation's information handling activities to ensure compliance with law and guidance; • ensure staff are sufficiently trained to support their role; • ensure that the organisation submits their annual IG Toolkit Assessment; • support monitoring visits from the commissioning organisation (where appropriate).

Creating an Improvement Plan

11. A duty of the Information Governance Lead is to develop a locally tailored IG improvement plan which documents both the current level of compliance with the NHS IG requirements and the targets that have been identified to progress to the next level of compliance.

12. To create the improvement plan, there is a need to work through each IG Toolkit requirement and consider the current compliance status and next steps to improve compliance. By setting targets and entering comments within the Information Governance Toolkit (IGT) an improvement plan can be automatically generated. As evidence of completed work is accumulated details should be entered into the IGT and the compliance level will be automatically updated.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
The National Health Service (Pharmaceutical Services) Regulations 2005	Regulations for the provision of pharmaceutical services which came into force on 1st April 2005.	24/01/2013
The National Health Service (General Dental Services Contracts) Regulations 2005	Regulations for the provision of dental services which came into force on 1st January 2006.	24/01/2013
The National Health Service (General Medical Services Contracts) Regulations 2004	Regulations for the provision of general medical services which came into force on 1st March 2004.	24/01/2013

The National Health Service (General Ophthalmic Services Contracts) Regulations 2008	Regulations for the provision of ophthalmic services which came into force on 1st August 2008.	24/01/2013
DH: What You Should Know About Information Governance Booklet	A 12 page booklet published by the Department of Health in July 2010 explaining Information Governance.	24/01/2013
HSCIC: Good Practice Guidelines in Information Governance - Information Security	The Good Practice Guidelines (GPG) are a series of informational documents which provide best practice advice in technology specific areas of Information Security.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Dental practice template: IG Work Plan (XLS, 109 KB)	A template work plan enabling details to be entered about current and target IGT scores, and the work required to make improvements. This has been developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
Pharmacy template: IG Workplan (DOC, 39 KB)	A template work plan enabling details to be entered about current and target IGT scores, and the work required to make improvements. This has been developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, DH and IG leads in the NHS.	24/01/2013
Wandsworth Teaching PCT: IG Report to Trust Board (DOC, 136 KB)	A review of Information Governance accountability arrangements that documents the current governance arrangements for Information Governance and improvement actions to address identified gaps and weaknesses.	24/01/2013
DH: Job Description - General Practice IG Lead (DOC, 88 KB)	To provide General Practices with examples of the qualities, experience and knowledge needed of an Information Governance Lead.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Information Governance Web Pages	These pages contain policy, guidance, publications and links to materials on all aspects of information governance.	24/01/2013
Pharmaceutical Services Negotiating Committee: IG Web Pages	Information for community pharmacy on NHS Information Governance - the IG training booklet can be downloaded from this site.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **Introduction to IG for General Practice Staff** - an introductory level module aimed at all general practice staff to inform them about good Information Governance.
- **Introduction to IG for Dental Practice staff** - an introductory level module aimed at all dental practice staff to inform them about good Information Governance.
- **Introduction to IG for Community Pharmacy** - an introductory level module aimed at community pharmacy staff to inform them about good Information Governance.
- **The role of the Caldicott/IG Lead in General Practice** - an introductory level module that explores the role of the Caldicott/IG Lead, its importance to the Practice and the support available.
- **The Caldicott Guardian in the NHS and Social Care** - a practitioner level module aimed at newly appointed Caldicott Guardians and those needing to know more about the role of the Caldicott Guardian.
- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of information risk management. Staff whose roles involve the handling of personal data will benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.
- **Password Management** - an introductory module on protecting sensitive data by choosing a good password.
- **Information Security Guidelines** - an introductory module on keeping information secure in and out of the workplace.
- **Secure Transfers of Personal Data** - a foundation level module that informs learners how to protect sensitive data from unauthorised access and

accidental loss, damage or destruction during transfer and how to dispose of sensitive data when it is no longer needed.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- Department of Health Information Governance Policy
- Care Quality Commission: Standards for better health
- NHS Pharmaceutical Regulations 2005: Schedule 1, Part 4, s26(2)(f) a use of information programme
- The National Health Service (General Dental Services Contracts) Regulations 2005, Part 5, section 33; and the National Health Service (Personal Dental Services Agreements) Regulations 2005, Part 5, section 34 - Confidentiality of personal data
- National Health Service England General Ophthalmic Services Contracts Regulations 2008; Schedule 1, Part 4 Confidentiality of personal data, Para 12
- The National Health Service (General Medical Services Contracts) Regulations 2004 section 75 - Confidentiality of personal data
- Corporate governance framework for PCTs 2003 (includes links to all organisation types)
- Integrated governance handbook 2006: A handbook for executives and nonexecutives in healthcare organisations

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**Responsibility for Information Governance has been assigned and an IG improvement plan has been developed.**		
	a	Responsibility has been assigned for Information Governance. **Evidence Required:** • Named individual(s) job description(s), or a signed note or e-mail assigning responsibility.	❑
		Notes/other evidence:	
	b	The named Information Governance staff have been provided with sufficient training to carry out their role. **Evidence Required:** • IG Training Tool reports, certificates of attendance and attainment, or evidence of self-directed study.	❑
		Notes/other evidence:	
	c	There is an IG improvement plan that documents both the current level of compliance with the NHS IG requirements and the targets identified to progress to the next level of compliance. **Evidence Required:** • Documented IG improvement plan.	❑
		Notes/other evidence:	
2	**The IG improvement plan has been approved by a senior staff member and is being implemented.**		
	a	The IG improvement plan has been signed-off by a senior staff member. **Evidence Required:** • Sign off should be documented on the IG improvement plan, for example the date that it was signed-off and by whom.	❑
		Notes/other evidence:	
	b	The IG improvement plan has been implemented and gaps or weaknesses in current IG arrangements are being addressed. **Evidence Required:** • New guidance for staff or new organisational procedures or new ways of working.	❑
		Notes/other evidence:	

3	**In-year reports and briefings on progress against the improvement plan are provided to senior management. IG arrangements are reviewed by a senior member of the organisation on at least an annual basis.**		
	a	Progress against the improvement plan is monitored in-year and reports are made to senior members of staff. **Evidence Required:** • Progress reports or briefing documents or meeting notes or emails.	❑
		Notes/other evidence:	
	b	[Level 3 Maintenance - only required if Level 3 achieved in previous year] The adequacy of the IG arrangements needs to be reviewed at least annually to ensure they remain fit for purpose. **Evidence Required:** • Minutes/meeting notes including the decisions made and any changes required.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

There is an information governance policy that addresses the overall requirements of information governance	Requirement No:	11-115
	Initiative:	Information Governance Management
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

There is a need to ensure that everyone working for or on behalf of the organisation (including temps, volunteers, locums and students) is aware of the organisation's overall approach to IG and where underpinning procedures and processes can be found. This can be achieved by developing an Information Governance policy.

Information Governance Policy Document

Introduction

1. Each organisation is required to have an Information Governance policy which is a high level statement of its intended approach to effectively implementing Information Governance. The policy should outline the procedures in place, or to be put in place, underpinning the policy, set out what is expected of staff in order to ensure compliance and should be reflective of national NHS information governance guidance.

Developing the Policy

2. Responsibility for developing and/or maintaining the currency of the policy sits with the organisation's *Information Governance Lead* and should be agreed by a senior management member of the organisation, for example the owner, NHS contractor, partner or other senior person.
3. Best practice requires that the policy is regularly reviewed and updated in the light of that review. Any amendments to the policy over time also must be signed off by a senior representative.
4. Template policies can be found in the **Knowledge Base Resources**. Each organisation should decide whether one of the templates is sufficient for its needs and, if so, adopt or amend the template as necessary. For example, the organisation should consider whether the template:
    - reflects the way in which information is handled within the organisation;
    - requires any amendment/removal of non-applicable detail;
    - requires any additions to reflect differing internal procedures.
5. Organisations are of course free to develop their own IG policy ensuring that all procedures referenced within it are relevant to its needs.

Table 1: Suggested key content of an Information Governance policy
• a section specifying why the policy is required – ie to safeguard the movement of personal identifiable data in the organisation; • an overview of how information will be handled by the organisation – maintenance of confidentiality, safe havens, storage of data, consent to view data, situations where disclosure may be required; • a description of accountability and responsibility for the policy – ie details of who is the IG lead in the organisation and job roles of any support staff; • a process for monitoring the policy; • staff duties and responsibilities for information governance (maintaining confidentiality of data, ensuring secure storage of data, being aware of situations where disclosure may be required); • a description of how the various areas within the policy link together; • actions to be taken if the policy is breached – ie sanctions against staff, remedial work on the part of those responsible for IG procedure.

6. The policy should be made available to all staff members, including administrative staff. Particular attention should be drawn to the section of the policy setting out staff responsibilities for compliance and also to the procedures that underpin the policy.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
DH: NHS Operating Framework for England for 2010/11 (PDF, 914 KB)	The Operating Framework for the NHS for 2010/11 sets out the priorities for the NHS for the year ahead to enable them to begin their planning. The Operating Framework 2010/11 confirms that informatics will be included in operational plans and this document provides guidance on the informatics components of these plans. National expectations for the NHS for delivery of national and local objectives are set out, building on existing investments to strengthen local information and data management.	24/01/2013
DH: Informatics Planning 2010/2011 (PDF, 913 KB)	This Informatics Planning guidance is published alongside the NHS Operating Framework for 2010/11, to provide detailed guidance regarding the informatics elements of local operating plans.	24/01/2013

Confidentiality NHS Code of Practice 2003	The Code is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their information.	24/01/2013
DH: Records Management NHS Code of Practice 2008	The Code is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The guidance applies to all NHS records and contains details of the recommended minimum retention period for each record type.	24/01/2013
DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013
The National Health Service (Pharmaceutical Services) Regulations 2005	Regulations for the provision of pharmaceutical services which came into force on 1st April 2005.	24/01/2013
General Pharmaceutical Council: Conduct, Ethics and Performance	The Code of Ethics applies to both pharmacists and pharmacy technicians. It is published with supporting professional standards and guidance documents that have been developed to expand upon the principles of the Code for specific areas of practice or professional activities.	24/01/2013
General Dental Council: Standards for Dental Professionals	The GDC produced and published its core guidance, Standards for Dental Professionals in 2005. This booklet, and the supplementary guidance booklets and statements which support it, lists the principles and values within which dental practitioners should operate.	24/01/2013

General Optical Council: Code of Conduct for Business Registrants	This document describes principles of good practice in professional conduct and standards and sets out a framework of conduct expected of all bodies corporate carrying on business as an optometrist, or a dispensing optician or both.	24/01/2013
College of Optometrists: Code of Ethics and Guidelines for Professional Conduct	The Code of Ethics is the basis of the whole professional conduct of optometrists, and all Fellows and Members of the College must subscribe to it.	24/01/2013
General Medical Council: Confidentiality 2009	Confidentiality (2009) sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. Supplementary guidance explaining how these principles apply in situations doctors often encounter or find hard to deal with is also available.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Pharmacy template: Information Governance Policy (DOC, 41 KB)	A template IG policy developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, the Department of Health and IG leads in the NHS.	24/01/2013
Pharmacy template: Staff Signature List (DOC, 45 KB)	A template for staff to sign to confirm their understanding of the responsibilities they carry for the proper handling of confidential patient information. Developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, the Department of Health and IG leads in the NHS.	24/01/2013
GP Information Governance policy (DOC, 32 KB)	An exemplar to assist general practices to define their own IG policy.	24/01/2013
DH: NHS IG - Staff Declaration Form (DOC, 59 KB)	A form for staff to sign to confirm that they have received information and guidelines regarding information governance in their organisation.	24/01/2013

Dental practice template: Information Governance Policy (DOC, 51 KB)	A template IG policy developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
Dental practice template: Staff Declaration Form (DOC, 57 KB)	A form for staff to sign to confirm that they have received information and guidelines regarding information governance in the practice, developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
Trust Information Governance Policy (DOC, 42 KB)	An exemplar to assist organisations to define their own IG policy.	24/01/2013
Voluntary Sector Template: YPAS Line Management Supervision Policy (DOC, 187 KB)	Template Line Management Supervision Policy for use by voluntary sector organisations.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Information Governance Web Pages	These pages contain policy, guidance, publications and links to materials on all aspects of information governance.	24/01/2013
General Practice - Data Quality Support (QOF)	To help GPs to find material relevant to their work, GP2GP, GP Systems of Choice, Quality Management and Analysis System and Quality and Outcomes Framework are grouped together here, in one section.	24/01/2013
Pharmaceutical Services Negotiating Committee: IG Web Pages	Information for community pharmacy on NHS Information Governance - the IG training booklet can be downloaded from this site.	24/01/2013

Requirement Origins

- Department of Health Information Governance Policy
- Protecting and using patient information: a manual for Caldicott Guardians 1999
- The Lord Chancellor's code of practice on the management of records, issued under section 46 of the Freedom of Information Act 2000, published November 2002
- Care Quality Commission: Standards for better health

- NHS Pharmaceutical Regulations 2005: Schedule 1, Part 4, s26(2)(f) a use of information programme
- Royal Pharmaceutical Society of Great Britain (RPSGB) Professional standards and guidance for pharmacists PS 2 Policies and procedures: Standard 2.7
- RPSGB Professional standards and guidance for patient confidentiality PS 2 Keeping information confidential: Standard 2.6 Standard Operating Procedures
- General Dental Council (GDC) Standards for dental professionals Standard 3 Protecting the confidentiality of patients' information Sections 3.1, 3.2 and 3.3
- General Optical Council - Code of conduct for business registrants, Principle 5
- College of Optometrists - Code of Ethics and Guidelines for Professional Conduct: A9 Patient Records
- General Medical Council (GMC) Good Medical Practice
- General Medical Council (GMC) Confidentiality 2009 paragraph 12
- Corporate governance framework for PCTs 2003 (includes links to all organisation-types)
- Integrated governance handbook 2006: A handbook for executives and nonexecutives in healthcare organisations

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**Current policies have been reviewed to determine where they can be adapted to form the basis of an Information Governance policy, which should underpin the organisation's IG improvement plan (see requirement 10-114).**		
	a	The IG lead(s) has/have reviewed current policies to determine where they can be adapted to form the basis of an Information Governance policy. **Evidence Required:** • An IG policy document tailored to the requirements of the organisation.	❑
		Notes/other evidence:	
	b	The IG policy has been signed off by a senior member of the organisation. **Evidence Required:** • Sign off documented on the policy document (for example - the date that it was signed-off and by whom).	❑
		Notes/other evidence:	
2	**The approved IG policy has been made available to all members of the organisation's staff.**		
	a	The IG policy has been made available to all members of organisation's staff. **Evidence Required:** • Inclusion in a staff handbook or by placing it on the Intranet, or staff may be provided with their own copy of the policy. In the latter case there may be a list of staff signatures confirming staff have read and understood the policy.	❑
		Notes/other evidence:	
3	**Staff compliance with the IG policy is monitored and assured.**		
	a	Staff understanding of the policy and its relevance to the way they work is tested to ensure that there is full compliance with the IG policy. Therefore, compliance spot checks and routine monitoring are conducted. **Evidence Required:** • Completed monitoring form, or a report on the outcome of staff compliance checks.	❑
		Notes/other evidence:	

	b	[Level 3 Maintenance - only required if Level 3 achieved in previous year] The adequacy of the IG policy needs to be reviewed regularly to ensure it remains fit for purpose. **Evidence Required:** • Minutes/meeting notes including the decisions made and any changes required.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

All contracts (staff, contractor and third party) contain clauses that clearly identify information governance responsibilities	Requirement No:	11-116
	Initiative:	Information Governance Management
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

One of the ways in which an organisation can ensure it fulfils its legal and other responsibilities regarding confidential information is to ensure that all staff members (including temps, locums, students and volunteers) are fully informed of their own obligations to comply with information governance requirements.

Contractual Clauses

Introduction

1. All organisations have a common law duty as well as a specific requirement under the *Data Protection Act 1998* to ensure that confidential information is processed lawfully and protected from inappropriate disclosure. Breach of confidence, inappropriate use of patient/service user records or abuse of computer systems may lead to disciplinary measures including for NHS contractors, loss of their NHS contract.
2. Fulfilling the organisational duties necessarily requires that everyone working for or on behalf of the organisation complies with information governance requirements. **References to staff members therefore includes employees, temporary and bank staff, locums, volunteers, students on placement etc**. It is preferable that there is a specific and explicit clause in the contract of employment, volunteer agreement or contract for services (eg IT services) stating an obligation to keep personal information confidential; otherwise, the organisation may have little or no defence in the event of an accidental or intentional breach by a member of staff or third party. The contract will also provide a formal record that an organisation has taken steps to ensure that staff recognise their own responsibility for protecting health and care information.
3. Although setting out the responsibilities of staff members will not automatically absolve the organisation of all blame, it will clearly be of assistance should a member of staff deliberately and intentionally, or recklessly, breach the law.

Professional Obligations

4. All healthcare professionals also have an obligation to comply with the standards for confidentiality and records' keeping set by their respective professional bodies.
5. For example:

- dentists and registered members of the dental team, ie clinical dental technicians; dental hygienists, dental nurses, dental technicians, dental therapists, and orthodontic therapists must comply with the General Dental Council Principles for Patient Confidentiality;
- general practitioners are licensed to practice by the General Medical Council and must comply with the standards the Council sets for professional practice;
- Pharmacy professionals must comply with the standards set out by the General Pharmaceutical Council.
- dispensing appliance contractors that are members of the British Health Trades Association must comply with the BHTA Code of Practice: British Health Trades Association website
- registered nurses employed by dispensing appliance contractors or general practice must comply with the standards of conduct, performance and ethics published in the Nursing and Midwifery Council Code

6. Failure to adhere to these standards could form the basis of a complaint of professional misconduct.

Content of the Clause

7. Ideally, the contract clause should reference the organisation's staff confidentiality code of conduct (where a code is required, see IG Toolkit **requirement 201** or **214** dependent on organisation type) as a source of further information about how the organisation expects its staff to behave in respect of maintaining the confidentiality and security of health and care information.

Table 1: Suggested Contract Clause for Individual Staff Members:
You may not during or after the termination of your employment disclose to anyone other than in the proper course of your employment or where required by law, any information of a confidential nature relating to the company or its business or customers. Breach of this clause may lead to dismissal without notice. Guidance on standards expected can be found in the staff code of conduct.

8. For staff members that don't have a contract of employment, for example locums, volunteers or university students on temporary placement, organisations should put in place an agreement which obligates the individuals to safeguard personal information and makes reference to the 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.

9. For third parties, care needs to be taken to ensure there are appropriate confidentiality and non-disclosure clauses in contracts with suppliers and service providers where they may have access to personal or sensitive information. This will include those third parties who may incidentally have access, (eg cleaners) and those with access to the systems which hold such information (eg IT system suppliers or software support).

   Detailed guidance on addressing security in third party agreements is available in paragraphs 14 - 23 below.

Ensuring Compliance

10. To support compliance with these obligations, organisations must ensure that contracts with staff, contractors and third parties contain clauses which clearly set out their responsibilities for ensuring and maintaining good information governance practice.

11. Initially an organisation should undertake an audit of personnel records, contractor and other third party contracts and determine how many have written contracts, and of those, which contain clauses that identify responsibilities for information governance, linked to disciplinary procedures (where appropriate).

12. Where gaps exist, a process should be implemented to ensure that appropriately worded clauses are issued to, signed and incorporated within the contracts of existing staff, contractor and third parties; and all new members of staff and new contracted third parties sign a contract containing an IG clause.

13. Guidance on what might be appropriate can be found in the **Knowledge Base Resources**.

Addressing Security in Third Party Agreements

14. Most organisations will have individuals from third party companies gaining access to their assets or premises. These might include:

    - other healthcare professionals;
    - contract cleaners;
    - security consultants;
    - auditors and accountants;
    - IT suppliers.

15. It is essential that these third parties are made aware of information governance requirements; what they can and cannot do, and who they should contact if things go wrong.

16. An organisation should conduct a full risk assessment to determine any potential threats to networks, systems and locations from third party operatives.

17. The extent of the risk assessment should be appropriate for the role of the third party contractor. For example, a risk assessment for cleaning contractors will be different to that carried out for an IT contractor connecting to the organisation's network. Temporary access will also see different considerations to long-term access. It is essential that the nature and level of access is determined before the risk assessment is conducted and before the information governance elements of the contract are completed.

18. It is also essential to know what safeguards the third party has in place. For example does the third party:

    - have adequate security controls, policies and training?
    - screen their staff?
    - have the necessary skills to train their staff in information governance issues?

19. If not, the organisation should agree training and awareness requirements with the third party.

20. The organisation must take all reasonable steps to ensure that the contractors and support organisations to whom personal information is disclosed comply with their contractual obligations to keep personal information secure and confidential. **Contracts with 3rd party data recipients must include a clause requiring incidents to be reported to the data provider**.

21. Table 2 outlines the key components of third party non-disclosure agreements.

Table 2: Key components of third party non-disclosure agreements
Specific reference to Data Protection and security issues, such as: • notification of the fact of processing data to the *Information Commissioner's Office*; • obligations to comply with limits set by the organisation; • the security and data protection standards that apply to both parties; • whether the contractor can act independently or only on instruction from the organisation
Specific reference to freedom of information issues, such as: • duty to disclose; • exemption from disclosure provisions; • records management processes; • responsibility for freedom of information applications.
Additionally: • penalties for breach of the non-disclosure agreement; • a provision to indemnify the organisation against breaches by the third party; • responsibilities for costs, eg for security audit, subject access, for handling information requests; • Incident-reporting requirements, **contracts with 3rd party data recipients must include a clause requiring incidents to be reported to the data provider**.

22. There should be a mechanism in place that provides the organisation with assurance that information governance requirements have been met. For third party contractors, this could take the form of viewing the third party contractor's security policies, procedures or controls to ensure they are acceptable, complete and up to date. Alternatively, the contractor could sign to confirm they adopt the organisation's own information governance policies and procedures or an independent assurance certificate could be provided by the contractor (for example, an *ISO 27001* certificate).

23. Third party access may be granted to electronic systems and networks. For example, the software for a patient record system may be maintained by the system supplier, under contract. In this case it is quite likely that the supplier's staff will have significant access to personal data. Care needs to be taken to ensure there are appropriate confidentiality and non-disclosure clauses in these contracts.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
Confidentiality NHS Code of Practice 2003	The Code is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their information.	24/01/2013
NHS Employers: Recruitment and Retention - Employment Checks	NHS Employers provides guidance and advice to NHS organisations on policies and procedures designed to prevent unsuitable people obtaining employment in the NHS. These web pages contain the NHS Employment Check Standards which outline the legal and mandated requirements for pre-employment checks in the NHS.	24/01/2013
NHS Employers: Identity Check Standards	All organisations are required to assure the identity of individuals involved in the provision of NHS services, for which that organisation is responsible as per the NHS Employment Check Standards April 2008 (Rev July 2010)	24/01/2013
The NHS Care Record Guarantee for England	The Guarantee sets out the rules that govern how patient information is used by all organisations providing care for or on behalf of the NHS and what control the patient can have over this.	24/01/2013
Joint IT Committee: The Good Practice Guidelines for GP electronic patient records Version 4 (2011) (PDF, 1732 KB)	The new Good Practice Guidelines for GP electronic patient records v4 (GPGv4 2011) will act as a reference source of information for all those involved in developing, deploying and using general practice IT systems.	24/01/2013
General Medical Council: Confidentiality 2009	Confidentiality (2009) sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. Supplementary guidance explaining how these principles apply in situations doctors often encounter or find hard to deal with is also available.	24/01/2013

General Pharmaceutical Council: Conduct, Ethics and Performance	The Code of Ethics applies to both pharmacists and pharmacy technicians. It is published with supporting professional standards and guidance documents that have been developed to expand upon the principles of the Code for specific areas of practice or professional activities.	24/01/2013
General Dental Council: Standards for Dental Professionals	The GDC produced and published its core guidance, Standards for Dental Professionals in 2005. This booklet, and the supplementary guidance booklets and statements which support it, lists the principles and values within which dental practitioners should operate.	24/01/2013
General Optical Council: Code of Conduct for Business Registrants	This document describes principles of good practice in professional conduct and standards and sets out a framework of conduct expected of all bodies corporate carrying on business as an optometrist, or a dispensing optician or both.	24/01/2013
College of Optometrists: Code of Ethics and Guidelines for Professional Conduct	The Code of Ethics is the basis of the whole professional conduct of optometrists, and all Fellows and Members of the College must subscribe to it.	24/01/2013
Directgov: Employment Contracts	Information about employment contracts, rights to a written statement of terms and other employment matters.	24/01/2013
Information Commissioner: Outsourcing - A Guide for Small and Medium Sized Businesses	This good practice note sets out what you need to do to comply with the Data Protection Act 1998 when you outsource the processing of personal information. Typical examples would include outsourcing your payroll function or customer mailings. It sets out which parts of the Act are important when outsourcing and provides some good practice recommendations.	24/01/2013
Data Protection Act 1998	The Act that makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
DH: Example Confidentiality Clauses (DOC, 25 KB)	Example contract clauses for individual staff members from the British Medical Association, the Law for Business Corporation Limited and others.	24/01/2013
Pharmacy template: Staff Confidentiality Agreement (DOC, 25 KB)	A template confidentiality agreement to be signed by individual staff developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, the Department of Health and IG leads in the NHS.	24/01/2013
Dental practice template: Confidentiality Agreement for Staff (DOC, 26 KB)	A template confidentiality agreement to be signed by individual staff developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
East Surrey: Confidentiality Clause for Staff Contracts 2002 (DOC, 35 KB)	Document setting out employee responsibilities for the confidentiality of personal information and the applicable legislation.	24/01/2013
IG Resource Pack	These useful resources comprise staff awareness leaflets, exemplars, templates and model documents. Practices should scroll down the page for GP requirement specific resources.	24/01/2013
Voluntary Sector Template: YPAS Confidentiality Agreement - 3rd Party Suppliers (DOC, 118 KB)	Template 3rd Party Suppliers Confidentiality agreement for use by voluntary sector organisations.	24/01/2013
Voluntary Sector Template: YPAS Confidentiality Policy (DOC, 192 KB)	Template Confidentiality Policy for use by Voluntary Sector organisations.	24/01/2013
Voluntary Sector Template: YPAS Disciplinary Policy (DOC, 186 KB)	Template Disciplinary policy for use by Voluntary Sector organisations.	24/01/2013

Voluntary Sector Template: YPAS Staff Confidentiality Agreement (DOC, 57 KB)	Template Staff Confidentiality Agreement for use by Voluntary Sector organisations.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Pharmaceutical Services Negotiating Committee: IG Web Pages	Information for community pharmacy on NHS Information Governance - the IG training booklet can be downloaded from this site.	24/01/2013
National Pharmacy Association: Home Page	National Pharmacy Association (NPA) members can obtain guidance on employment matters including employment contracts from the NPA Personnel Department.	24/01/2013
Information Commissioner: Home Page	The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.	24/01/2013

Requirement Origins

- Confidentiality NHS Code of Practice
- ISO/IEC 27002.2005 controls ref 6.2 & 10.2
- NHS Care Records Guarantee, Commitment 9
- Data Protection Act 1998, Principle 7
- Data Protection Act 1998, Schedule 1, Part II, Paragraph 11
- Protecting and using patient information, Caldicott management audit point 7
- Royal Pharmaceutical Society of Great Britain (RPSGB) Professional standards and guidance for pharmacists PS 4 Responsibilities to those you employ, manage or lead: Standard 4.3
- RPSGB Professional standards and guidance for patient confidentiality PS 2 Keeping information confidential: Standard 2.5
- General Dental Council (GDC) Standards for dental professionals, Standard 5 - Maintain your professional knowledge and competence: 5.4
- GDC - Guidance on Principles of Management Responsibility, Principle 1 - Your own behaviour: 1.3
- GDC - Guidance on Principles of Management Responsibility, Principle 2 - The behaviour of other people within your organisation: 2.2
- GDC - Principles of Dental Team Working, Principle 5 - Leading a team: 5.4
- General Optical Council - Code of conduct for business registrants, Principle 2

- College of Optometrists - Code of Ethics and Guidelines for Professional Conduct: A02 - The patient-practitioner relationship; A05 - Inter-and intra-professional relationships
- General Medical Council (GMC) Confidentiality 2009 paragraph 12

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**Action has been taken to determine whether contracts of staff, contractors and third parties contain clauses setting out IG responsibilities.**		
	a	An audit of personnel records, and contractor and other third party contracts has been undertaken to determine how many have written contracts that contain clauses that identify IG responsibilities. **Evidence Required:** • A list of staff (including temps, locums, students and volunteers), contractors and third parties with access to personal information.	❑
		Notes/other evidence:	
	b	Appropriate contractual clauses covering compliance with IG linked to disciplinary procedures (where appropriate) have been drafted and signed off by senior management. **Evidence Required:** • Examples of contract clauses. • Meeting notes showing approval or personal endorsement in writing (eg by email) from an appropriate senior manager.	❑
		Notes/other evidence:	
	c	An action plan has been developed to update existing contracts, where necessary, and ensure all new contracts include compliance with IG requirements as part of employment/service engagement processes. **Evidence Required:** • Documented action plan.	❑
		Notes/other evidence:	
2	**Appropriate clauses on compliance with IG have been put into all contracts and/or agreements.**		
	a	Building upon the existing contractual situation, all contracts for staff, contractors and other third party users who have access to confidential information or assets containing confidential information include compliance with information governance requirements, as part of employment or contracting processes. **Evidence Required:** • Sample contract showing that appropriate IG clauses are included in contracts.	❑
		Notes/other evidence:	

3	**Compliance with the clauses is monitored and assured. Formal contractual arrangements with staff, contractors and third parties are reviewed regularly.**		
	a	All new staff, contractor and other third parties comply with IG responsibilities and this is tested through spot checks and routine monitoring. **Evidence Required:** • Completed monitoring forms, or a report on the outcome of staff compliance checks.	❑
		Notes/other evidence:	
	b	[Level 3 Maintenance - only required if Level 3 achieved in previous year] As the law in this area is subject to change, an annual review is undertaken to assess whether the contractual clauses are still sufficient. **Evidence Required:** • Meeting notes including the decisions made and any changes required.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

All staff members are provided with appropriate training on information governance requirements	Requirement No:	11-117
	Initiative:	Information Governance Management
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

To maintain information handling standards in the organisation staff should be provided with appropriate training on information governance.

Information Governance Awareness and Training

Introduction

1. It is essential that everyone working for or on behalf of the organisation is fully informed about Information Governance (IG) procedures and in particular given clear guidelines about their own individual responsibilities for maintenance of good IG practice.

Ensuring Staff are Effectively Informed about Information Governance

2. Therefore, measures should be put in place to ensure that all staff members are fully informed of the procedures implemented to ensure Information Governance requirements are met.
3. The organisation should ensure that appropriate IG training is made available to all staff, including temps, locums and volunteers. There should be a clearly documented and communicated process for making all staff aware of the availability and importance of training.
    a. All staff should be provided with basic IG awareness training and informed where support and further information are available. Particular emphasis should be placed on how the requirements affect their day to day work practices.
    b. All staff members who have routine access to confidential information should be provided with additional IG training.
    c. Ideally all new staff members should be provided with IG training within a short time of taking on their post.

Training Needs Assessment

4. To identify appropriate training, a training needs assessment could be carried out. Such an assessment will generally consist of the following steps:
    - an assessment of the skills and competencies required to perform a particular job, with emphasis on the importance of that skill-set to the job;

- an assessment of the current level of skills and competencies of the staff member performing the job;
- a comparison of the two assessments and identification of any gaps between the two, ie does the person performing the role have, or have access to a person with, sufficient skill and knowledge to enable successful performance;
- identification of appropriate training to meet the skills/competency gap.

5. Training needs analyses also allow an organisation to plan regular training programmes in the future where the skills gap identified is a common theme.

Training Products

6. The Pharmaceutical Services Negotiating Committee (PSNC) and the Royal Pharmaceutical Society for Great Britain worked with Department of Health 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.

7. The NHS undertakes mandatory training using the NHS Information Governance Training Tool (or equivalent centrally approved materials) which provides a valuable base on which to build. E-learning modules have also been developed specifically for community pharmacy, dental practices and general practices.

8. The IG Training Tool comprises a structured e-learning programme with Introductory, Foundation and Practitioner level modules covering all aspects of IG. The organisation needs to be registered in the Tool before users can set up an account, and ideally an organisation administrator should be nominated and given the appropriate permissions to monitor staff training. This can all be arranged by logging a request with the IG Training Tool Helpdesk at CFH.IG-trainingtoolhelpdesk@nhs.net and providing the organisation name, corporate email domain (if one exists) and ODS code, (also known as the practice code, the national code, or the pharmacy F code found on the submission document used to send prescriptions to NHS Prescription Services).

9. Once the organisation is registered, other members of staff will be able to register on the Tool. As part of the user registration process, staff will be asked for their organisation's ODS code, so it is important to ensure staff know what the code is before they attempt to register. If no corporate email domain exists, staff can still register by selecting "no" when asked if they have a work email and following the steps to create an onscreen account.

10. Other equivalent training resources may also be used to meet this requirement, for example in-house training packages produced by multiple premises organisations, or where available, training provided by a hosting or *commissioning organisation*.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
Confidentiality NHS Code of Practice 2003	The Code is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their information.	24/01/2013
General Medical Council: Good Medical Practice	Good Medical Practice sets out the principles and values on which good practice is founded; these principles together describe medical professionalism in action. There are links to other GMC guidance and information which illustrate how the principles in Good Medical Practice apply in practice, and how they may be interpreted in other contexts.	24/01/2013
General Medical Council: Confidentiality 2009	Confidentiality (2009) sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. Supplementary guidance explaining how these principles apply in situations doctors often encounter or find hard to deal with is also available.	24/01/2013
Joint IT Committee: The Good Practice Guidelines for GP electronic patient records Version 4 (2011) (PDF, 1732 KB)	The new Good Practice Guidelines for GP electronic patient records v4 (GPGv4 2011) will act as a reference source of information for all those involved in developing, deploying and using general practice IT systems.	24/01/2013
DH: Prison Health Induction Framework (PDF, 90 KB)	This framework is intended to form the skeleton of a short induction programme specifically for healthcare staff working in prisons.	24/01/2013
Information Commissioner: Training checklist for small and medium sized organisations (PDF, 34 KB)	This Data Protection Good Practice Note outlines some of the practical implications of the Act and is intended as a basic training framework for general office staff in small and medium sized organisations.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Pharmaceutical Services Negotiating Committee: IG Web Pages	Information for community pharmacy on NHS Information Governance - the IG training booklet can be downloaded from this site.	24/01/2013
HSCIC: Training Needs Analysis Supporting Guidance	This ETD standard and supporting guidance documents will help organisations to prepare for and complete a TNA for a project, department or organisation. A number of templates are available to support the development of in-house TNAs.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **Introduction to IG for General Practice Staff** - an introductory level module aimed at all general practice staff to inform them about good Information Governance.
- **Introduction to IG for Dental Practice staff** - an introductory level module aimed at all dental practice staff to inform them about good Information Governance.
- **Introduction to IG for Community Pharmacy** - an introductory level module aimed at community pharmacy staff to inform them about good Information Governance.
- **Password Management** - an introductory module on protecting sensitive data by choosing a good password.
- **Information Security Guidelines** - an introductory module on keeping information secure in and out of the workplace.
- **Information Governance: The Beginner's Guide** - an introductory level module that explains the importance of information governance to staff who do not generally require access to personal information.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.

- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- Confidentiality NHS Code of Practice
- Data Protection Act 1998 Schedule 1, Part II - Interpretation of Principle 7
- Royal Pharmaceutical Society of Great Britain (RPSGB) Professional standards and guidance for pharmacists PS 4 Responsibilities to those you employ, manage or lead: Standard 4.3
- RPSGB Professional standards and guidance for patient confidentiality PS 2 Keeping information confidential: Standard 2.5 Pharmacy staff
- General Dental Council (GDC) Standards for dental professionals, Standard 5 - Maintain your professional knowledge and competence: 5.4
- GDC - Guidance on Principles of Management Responsibility, Principle 1 - Your own behaviour: 1.3
- GDC - Guidance on Principles of Management Responsibility, Principle 2 - The behaviour of other people within your organisation: 2.2
- GDC - Principles of Dental Team Working, Principle 5 - Leading a team: 5.4
- College of Optometrists - Code of Ethics and Guidelines for Professional Conduct: A02 - The patient-practitioner relationship; A05 - Inter-and intra-professional relationships
- Confidentiality and Disclosure of Information: General Medical Services (GMS), Personal Medical Services (PMS), AND Alternative Provider Medical Services (APMS) Code of Practice paragraph 17 (i)
- Corporate governance framework for PCTs 2003 (includes links to all organisation types)
- Integrated governance handbook 2006: A handbook for executives and nonexecutives in healthcare organisations

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**Appropriate IG training has been identified that includes induction for new starters.**		
	a	Responsibility for arranging appropriate IG training for all staff has been assigned to a named individual. **Evidence Required:** • A named individual's job description, or a signed note or e-mail assigning responsibility.	❑
		Notes/other evidence:	
	b	Appropriate basic IG training has been identified for all staff including new starters, and additional training has been identified for key staff groups. **Evidence Required:** • Written details of the training to be provided.	❑
		Notes/other evidence:	
	c	Basic IG training is provided to all new starters as part of their induction. **Evidence Required:** • Training records, for example, IG Training Tool reports.	❑
		Notes/other evidence:	
2	**All staff members have completed or are in the process of completing IG training. Training needs are regularly reviewed and re-evaluated when necessary.**		
	a	All staff including locum, temporary, volunteer, student and contract staff members have completed or are in the process of completing basic IG training. **Evidence Required:** • Training reports or certificates of attendance.	❑
		Notes/other evidence:	
	b	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 which may be provided through the NHS IG Training Tool or by other means. **Evidence Required:** • Training needs analysis document, certificates of attendance / attainment or IG Training Tool reports.	❑
		Notes/other evidence:	

3	**Action is taken to test and follow up staff understanding of IG and additional support is provided where needs are identified. Training provision is regularly reviewed.**		
	a	Providing staff with IG training does not provide sufficient assurance that they have understood their IG responsibilities. Therefore, compliance checks and routine monitoring is undertaken to test staff understanding and to ensure procedures are being complied with, where necessary, actions are taken. **Evidence Required:** • A completed audit sheet or monitoring form, or a report on the outcome of staff compliance checks and any actions taken.	❑
		Notes/other evidence:	
	b	Where necessary, any staff member requiring assistance should be supported to increase their understanding of and adherence to IG best practice. **Evidence Required:** • Training attendance lists, diary slots for individual training, HR/personnel records, or in staff signature lists - that staff have received additional support and understand their duties and responsibilities.	❑
		Notes/other evidence:	
	c	[Level 3 Maintenance - only required if Level 3 achieved in previous year] Staff understanding and training materials are regularly reviewed especially when new procedures are introduced and on induction of new staff. **Evidence Required:** • Meeting notes where the training was reviewed during the year including the decisions made and any updates.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

Personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected	Requirement No:	11-202
	Initiative:	Confidentiality and Data Protection Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.1

Requirement Description

There are legal restrictions on how personal information may be used stemming from the *Data Protection Act 1998,* and where personal information is held in confidence (eg to provide care and treatment), the common law places additional constraints on its disclosure. Usually a form of consent is required, unless the disclosure is required by Court Order or under an *Act of Parliament*. Staff must be made aware of the right of an individual to restrict how confidential personal information is disclosed and the processes that they need to follow to ensure this right is respected.

Use and Disclosure of Personal Information

Introduction

1. The Data Protection Act 1998 provides conditions that must be satisfied prior to using or disclosing (both termed processing in the Act) personal information. Where personal information is held in confidence (eg health records or case file information) common law obligations additionally require the consent of the subject of the information before it is disclosed to a third party unless exceptional circumstances apply.

Data Protection Act 1998 Conditions

2. The Data Protection Act 1998 provides eight Principles that apply to all use and disclosure of personal information. In addition to satisfying these eight Principles, organisations must also satisfy one condition from a supplementary schedule and where the information is deemed sensitive under the provisions of the Act a further condition from a second supplementary schedule. These are explained in more detail in materials available from the **Knowledge Base Resources** but it is important to note that where a care organisation is using and disclosing personal information for purposes relating to the care of an individual the Act will not prevent that use or disclosure. However, other uses or disclosures are likely to require the explicit consent of the individual concerned.

Common Law Obligations

3. The Common Law requires that there is a lawful basis for the disclosure of personal information that is held in confidence. Unlike the Data Protection Act which applies to legal organisations in their entirety, the common law applies to the clinic, team

or workgroup caring for an individual, ie those not caring for the individual cannot assume they can access confidential information about the individual in a form that identifies them. Normally the basis of access will be consent which must be sought before disclosure of the information. It is generally accepted that this consent can be implied where the purpose is directly concerned with an individual's care or with the quality assurance of that care and the disclosure should not reasonably surprise the person concerned. The provision of information – see **requirement 203** depending on organisation type – is also important in this context to reinforce the basis for implying consent. The *Care Record Guarantee* (NHS and/or Social Care) sets out what service users have a right to expect. NB: Consent **cannot** be implied when an individual has expressly dissented.

4. In other circumstances and for other purposes consent cannot be implied and so must be specifically sought or there must be some other lawful basis for disclosing the information.

Using the Information for Purposes Unconnected to Care Services

5. Where an organisation wishes to disclose confidential personal information for a purpose unrelated to care, consent cannot be implied. In most cases, individuals should be asked for their explicit consent for information to be shared with non-care organisations, for example:

    - housing departments;
    - education services;
    - voluntary services;
    - Sure Start teams;
    - the police;
    - government departments.

6. Individuals must also be asked for explicit consent for their confidential personal information to be shared for non-care purposes, such as those in the Table 1.

Table 1: Non-care purposes
Checking quality of care • Testing the safety and effectiveness of new treatments and comparing the cost-effectiveness and quality of treatments in use; • Care audit activity on site; • Supporting Care Quality Commission audit studies; • Comparative performance analysis across clinical networks; and • Ensuring the needs of service users within special groups are being met eg children at risk, chronically sick, frail and elderly.

Protecting the health of the general public

- Drug surveillance (pharmacovigilance) and other research-based evidence to support the regulatory functions of the Medicines and Healthcare products Regulatory Agency;
- Surveillance of disease and exposures to environmental hazards or infections and immediate response to detected threats or events;
- Vaccine safety reviews;
- Safety monitoring of devices used in healthcare;
- Linking with existing National Registries for diseases / conditions;
- Analysis of outcomes following certain health interventions (ie public health interventions as well as treatments);
- Monitoring the incidence of ill health and identifying associated risk factors; and
- Identifying groups of patients most at risk of a condition that could benefit from targeted treatment or other intervention.

Managing care services

- Capacity and demand planning;
- Commissioning;
- Data for Standards and Performance Monitoring;
- National Service Frameworks;
- Clinical indicators;
- Information to support the work of the Care Quality Commission;
- Evidence to support the work of the National Institute for Health and Clinical Excellence;
- Measuring and monitoring waiting times, in support of the 18 week target;
- Data to support Productivity Initiatives;
- Agenda for Change; and
- Benchmarking.

Supporting research

- Assessing the feasibility of specific clinical trials designed to test the safety and/or effectiveness and/or cost-effectiveness of healthcare interventions;
- Identification of potential participants in specific clinical trials, to seek their consent;
- Providing data from routine care for analysis according to epidemiological principles, to identify trends and unusual patterns indicative of more detailed research; and
- Providing specific datasets for defined approved research projects.

7. Where explicit consent cannot be obtained the organisation may be able to rely on the public interest justification or defence. This is where the organisation believes that the reasons for disclosure are so important that they override the obligation of confidentiality (eg to prevent someone from being seriously harmed). There is more information on public interest disclosures available in a new annex to the Confidentiality: NHS Code of Practice. The new guidance can be downloaded from the **Knowledge Base Resources**.

8. Disclosure may also be required by Court Order or under an Act of Parliament, ie there is a statutory or other legal basis for the disclosure. Of particular note in this respect are disclosures permitted under *section 251* of the NHS Act 2006, formerly known as section 60 of the Health and Social Care Act 2001. Applications for

approval to use Section 251 powers are considered by the Ethics and Confidentiality Committee of the National Information Governance Board for Health and Social Care (NIGB).

9. The advice of specialist staff, eg *Caldicott Guardians* or legal advisors should be sought prior to making disclosures in the public interest or where a Court Order or statutory basis is provided as justification.

10. In general no-one may consent on behalf of another individual who has the capacity and competence to decide for themselves. However, treating clinicians, parents of young children, legal guardians, or people with powers under mental health law, eg the *Mental Capacity Act 2005* must make decisions that they believe are in the best interests of the person concerned.

11. It should also be borne in mind that an individual has the right to change their mind about a disclosure decision at any time before the disclosure is made, and can do so afterwards to prevent further disclosures where an activity requires a regular transfer of personal information.

The NHS and Social Care Record Guarantees for England

12. Individuals' rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

Staff Guidelines on Respecting Disclosure Decisions

13. To ensure individuals' rights to restrict disclosure of their personal information are respected, staff should be made aware of these rights and be provided with guidelines included in the organisation's confidentiality code of conduct or equivalent (see **requirement 201**). The guidelines should address:

    - where appropriate, the duty to comply with the commitments set out in the Care Record Guarantee (NHS and/or Social Care);
    - when and how consent should be obtained;
    - the basic premise that individuals have the right to choose whether or not to agree to the disclosure of their personal information;
    - the right of individuals to change their decision about a disclosure before it is made;
    - who should obtain consent for the further purpose;
    - where and how consent or dissent should be recorded;
    - answering questions about consent including how to provide information about the consequences of non-disclosure in a non-threatening, non-confrontational manner;
    - how often consent should be reviewed;
    - any sanctions for failure to respect individuals' disclosure decisions;
    - other lawful reasons for disclosure of confidential personal information - public interest, legally required and section 251 of the NHS Act 2006.

Services Provided by Third Parties

14. Where an organisation contracts with a third party to provide care services the contracts must prevent personal information from being used for purposes other than those contracted for and must also ensure that there is explicit consent or some other lawful basis where required.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
DH: Confidentiality NHS Code of Practice: Supplementary Guidance - Public Interest Disclosures 2010	Guidance to support the Confidentiality: NHS Code of Practice. The guidance is aimed at aiding decisions about disclosures of information in the public interest.	24/01/2013
Confidentiality NHS Code of Practice 2003	The Code is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their information.	24/01/2013
DH: The Caldicott Guardian Manual 2010	The manual is guidance that takes account of developments in information management in the NHS and in Councils with Social Services Responsibilities since the publication of the Caldicott report 1997. It sets out the role of the Caldicott Guardian within an organisational Caldicott/confidentiality function as a part of broader information governance.	24/01/2013
The NHS Care Record Guarantee for England	The Guarantee sets out the rules that govern how patient information is used by all organisations providing care for or on behalf of the NHS and what control the patient can have over this.	24/01/2013
The Social Care Record Guarantee for England	The Guarantee explains to service users how the information they provide to social care staff is used and what control they can have over this. It complements the NHS Care Record Guarantee for England.	24/01/2013

Information Commissioner: Health Sector specific guides provided by the ICO	The guidance provides practical examples of the steps that should be taken in order to achieve compliance with the requirements of the Data Protection Act 1998. The guidance is primarily for data protection officers, Caldicott Guardians and those charged with the development of the IT infrastructure of the NHS.	24/01/2013
HM Prison Service Standards Manual: Standard 37 - Personal Information (PDF, 102 KB)	Performance indicator for management of personal information by prison establishments and HQ.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Mid Essex Hospital: Photo Request card (PUB, 124 KB)	A card for recording patient consent to the taking of a clinical photograph and/or to use of the photograph for future research and/or publication in medical journals and/or for viewing by patients receiving similar treatment.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **The Caldicott Guardian in the NHS and Social Care** - a practitioner level module aimed at newly appointed Caldicott Guardians and those needing to know more about the role of the Caldicott Guardian.
- **Patient Confidentiality** - a foundation level module aimed at all NHS staff to gain an understanding of patient confidentiality and the role of the Caldicott Guardian in the NHS.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- The common law duty of confidence
- Data Protection Act 1998
- Confidentiality: NHS Code of Practice 2003

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**There are guidelines for staff on when it is both lawful and appropriate to share confidential personal information and on respecting service user wishes. The guidelines have been approved by senior management or an appropriate committee.**		
	a	Responsibility has been assigned for documenting guidelines for staff about lawful and appropriate sharing of confidential personal information and respecting service user wishes. **Evidence Required:** • A named individual's job description, a note or e-mail assigning responsibility or the terms of reference of a group.	❑
		Notes/other evidence:	
	b	The documented guidelines provide direction to staff to ensure they share confidential personal information lawfully and appropriately and that they respect service user choices regarding disclosure. **Evidence Required:** • A document, staff handbook, or leaflet covering consent issues around the use and disclosure of personal information.	❑
		Notes/other evidence:	
	c	The guidelines have been approved by senior management, an appropriate committee or other established local governance process. **Evidence Required:** • Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriately senior manager.	❑
		Notes/other evidence:	
2	**The documented and approved guidelines have been made available at appropriate points in the organisation and all staff members have been effectively informed about the need to comply with them.**		
	a	The guidelines for staff are accessible to them in an appropriate location. **Evidence Required:** • Inclusion in staff handbook, or published on the Intranet, or personal copies for staff (in the latter case there may be a list of staff signatures confirming receipt of the guidance) or the evidence may be a description of the dissemination process or minutes of the meeting where this was decided.	❑
		Notes/other evidence:	

	b	All staff members have been informed of the guidance and in particular of their own responsibilities for compliance. **Evidence Required:** • Notes or minutes of team meetings/awareness sessions or staff briefing materials.	❑
		Notes/other evidence:	
3	**Staff compliance with the guidelines is monitored to ensure, unless there is a legal reason not to, they respect service user choices when disclosing confidential personal information.**		
	a	Providing staff with guidance materials and briefings does not provide sufficient assurance that the guidance has been understood and is being followed, therefore compliance spot checks and routine monitoring are conducted. **Evidence Required:** • A completed monitoring form, or a report on the outcome of staff compliance checks. • Documentation from reviews of information sharing (eg where information has been shared for non-care services, where service users have declined to agree to disclosure or have changed their disclosure decision).	❑
		Notes/other evidence:	
	b	The purpose of staff following the guidelines is to ensure that information is shared in compliance with the law and is in line with the expectations of the public. Satisfaction surveys are used to check that service users understand their consent choices and feel that their wishes are respected. **Evidence Required:** • Completed satisfaction surveys.	❑
		Notes/other evidence:	
	c	[Level 3 Maintenance - only required if Level 3 achieved in previous year] Policy and law change over time and it is important that the content of guidance is regularly reviewed and aligned with the latest central guidelines. **Evidence Required:** • Minutes/meeting notes where the guidance has been reviewed during the year including the decisions made and any updates to the guidance.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

There are appropriate confidentiality audit procedures to monitor access to confidential personal information	Requirement No:	11-206
	Initiative:	Confidentiality and Data Protection Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.1

Requirement Description

Organisations should ensure that access to confidential personal information is monitored and audited locally and in particular ensure that there are agreed procedures for investigating confidentiality events.

Confidentiality Audit Procedures

Introduction

1. Good practice requires that all organisations that handle personal information put in place control mechanisms to manage and safeguard *confidentiality*, including mechanisms for highlighting problems such as *incidents*, complaints and alerts.
2. Organisations should have processes to highlight actual or potential *confidentiality breaches* in their systems, particularly where person identifiable information is held. They should also have procedures in place to evaluate the effectiveness of controls within these systems.

Purpose of the Confidentiality Audit

3. Confidentiality *audits* will focus primarily on controls within electronic records management systems, but should not exclude paper record systems: the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of weak, non-existent or poorly applied controls.
4. Assurances that these controls are working effectively should be part of the organisation's overall assurance framework and, as such, it is likely that many organisations are, at some level, already complying with this requirement. For example:
    - the IG Lead, Information Security Officer or equivalent may be undertaking reviews/follow ups of failed log-in reports provided for information systems;
    - *Caldicott Guardians*, IG Leads or equivalent may be monitoring incident reports regarding stolen/lost computers, disclosure of confidential material, complaints etc;

- internal audit processes may include reviews of IT security that cover such areas as records' systems to highlight allocation, use or abuse of passwords (indicating possible breach of access privileges).

5. It is important that those organisations who will in future be using the *NHS Care Records Service* (NHS CRS) think about how they currently obtain assurance on their confidentiality processes and how, and where, they need to improve on these in preparation for NHS CRS roll out.

Monitoring and Auditing Access to Confidential Information

6. The organisation should ensure that it has assigned overall responsibility for monitoring and auditing access to confidential personal information to an appropriate senior staff member, eg the Caldicott Guardian, IG Lead or equivalent. This member of staff should be responsible for ensuring that confidentiality audit procedures are developed and communicated to all staff with the potential to access confidential personal information. The procedures should include:

    - how access to confidential information will be monitored;
    - who will carry out the monitoring of access;
    - reporting processes and escalation processes;
    - disciplinary processes.

7. The following are examples of events that the organisation should audit for frequency, circumstances, location etc:

    - failed attempts to access confidential information;
    - repeated attempts to access confidential information;
    - successful access of confidential information by unauthorised persons;
    - evidence of shared login sessions/passwords;
    - disciplinary actions taken.

8. There are also alerts that are specific to the Summary Care Record (SCR) that can be viewed through the *TES Alert Viewer* system by an organisation's *Privacy Officer function*. The alerts are generated when:

    - A member of healthcare staff self-claims a Legitimate Relationship (LR) with the patient in order to view the patient's SCR.
    - A member of healthcare staff uses the emergency over-ride button to view the patient's SCR when the patient is unable to give Permission to View (PTV) eg if unconscious or confused.

Investigating Confidentiality Events and Alerts

9. The organisation should identify a senior manager, eg the Caldicott Guardian, *Senior Information Risk Owner*, IG Lead or equivalent to take responsibility for the investigation of confidentiality events.

10. The organisation should have a Privacy Officer function in place to take responsibility for auditing and monitoring SCR alerts. Organisations should decide how this function is best discharged and the way in which suspected inappropriate accesses are escalated in line with the local policy on confidentiality breaches.

11. The organisation also has a responsibility for providing appropriate support and training to enable the nominated individual(s) to carry out their role(s).

12. Investigation and management of confidentiality events and alerts should be in line with the management and reporting of serious untoward incidents – see **requirement 302** or **320** dependent on organisation-type.

13. Disciplinary procedures should outline the penalties for unauthorised access or attempts, eg suspension, supervised access to systems, ending a contract, firing an employee, or bringing criminal charges.

The NHS Care Record Guarantee for England

14. Individuals' rights regarding the sharing of their personal information are supported by the NHS *Care Record Guarantee*, which sets out high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
Care Quality Commission: Guidance about compliance with the Essential Standards	The essential standards of quality and safety are central to the Care Quality Commission's (CQC) work in regulating health and adult social care. Each of the standards has an associated outcome that CQC expects all people who use services to experience as a result of the care they receive. Outcome 21: Records, sets out the requirement for people's personal records, including medical records, to be accurate and kept safely and confidentially.	24/01/2013
The NHS Care Record Guarantee for England	The Guarantee sets out the rules that govern how patient information is used by all organisations providing care for or on behalf of the NHS and what control the patient can have over this.	24/01/2013

Information Commissioner: The Employment Practices Code (PDF, 449 KB)	This code is intended to help employers comply with the Data Protection Act and to encourage them to adopt good practice. The code aims to strike a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. It does not impose new legal obligations.	24/01/2013
HSCIC: Information Governance guidance for Privacy Officers and Caldicott Guardians on SCR alerts	Information for the Privacy Officer function in the NHS about understanding confidentiality audits and investigating alerts.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **The Caldicott Guardian in the NHS and Social Care** - a practitioner level module aimed at newly appointed Caldicott Guardians and those needing to know more about the role of the Caldicott Guardian.
- **Patient Confidentiality** - a foundation level module aimed at all NHS staff to gain an understanding of patient confidentiality and the role of the Caldicott Guardian in the NHS.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

ERROR: no requirement origins specified

Changes

The following is a list of *material* changes since the last major version of this requirement:

- Paragraphs 7, 9 and 10: additional guidance has been added regarding the types of alerts generated by the Summary Care Record (SCR) and how these should be managed and investigated.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**There are documented confidentiality audit procedures in place that include the assignment of responsibility for monitoring and auditing access to confidential personal information. The procedures have been approved by senior management or committee and have been made available throughout the organisation.**		
	a	Responsibility for documenting confidentiality audit procedures that cover monitoring and auditing access to confidential personal information has been assigned to an individual or group. **Evidence Required:** • A named individual's job description, a note or e-mail assigning responsibility or the terms of reference of a group.	❑
		Notes/other evidence:	
	b	There are documented confidentiality audit procedures that clearly set out responsibilities for monitoring and auditing access to confidential personal information. **Evidence Required:** • Documented confidentiality audit procedures which include the details of the named staff member, job role or responsible group.	❑
		Notes/other evidence:	
	c	The procedures have been approved by senior management, an appropriate committee or other established local governance process and have been made available throughout the organisation. **Evidence Required:** • Approval/sign off within the minutes of meetings, in a document or email or a personal endorsement in writing from an appropriately senior manager. • Inclusion in a staff handbook, or publishing the procedures on the Intranet or personal copies of the procedures provided to staff (in the latter case there may be a list of staff signatures confirming receipt of the procedures) or the evidence may be a description of the dissemination process or minutes of the meeting where the process was decided.	❑
		Notes/other evidence:	

2	**All staff members with the potential to access confidential personal information have been made aware of the procedures. The procedures have been implemented and appropriate action is taken where confidentiality processes have been breached.**		
	a	All staff members with the potential to access confidential personal information have been informed that monitoring and auditing of access is being carried out, of the need for compliance with confidentiality and security procedures and the sanctions for failure to comply. Staff might be informed through team meetings, awareness sessions, staff briefing materials, or staff may be provided with their own copy of the procedures. **Evidence Required:** • Minutes/notes of meetings, briefing and awareness session materials or a list of staff signatures that they have read, understood and will comply with the procedures.	❑
		Notes/other evidence:	
	b	The procedures have been effectively implemented and appropriate action is taken where confidentiality processes have been breached. Therefore staff compliance is monitored and there are case reviews if confidentiality processes have been breached. **Evidence Required:** • Completed monitoring form, or a report on the outcome of staff compliance checks. • Where a breach has occurred, copies of Serious Untoward Incident reports, lessons learned reports, staff feedback briefings, staff retraining files, or disciplinary documents. Evidence may also be found in public statements and communications to service users.	❑
		Notes/other evidence:	
3	**Access to confidential personal information is regularly reviewed. Where necessary, measures are put in place to reduce or eliminate frequently encountered confidentiality events.**		
	a	Access to confidential personal information is subject to regular review and, where necessary, measures are put in place to reduce or eliminate frequently encountered confidentiality events. **Evidence Required:** • Minutes/ meeting notes where access has been reviewed during the year including the decisions made such as new guidance for staff, improved physical security measures, documented IT system changes (eg stronger password formation; port control to prevent download of personal information to USB sticks, etc) or other new processes.	❑
		Notes/other evidence:	

	b	[Level 3 Maintenance - only required if Level 3 achieved in previous year] Policy and law change over time as do technological developments and it is important that the content of procedures is regularly reviewed, is aligned with the latest central guidelines and takes into account any new systems or processes introduced into the organisation. **Evidence Required:** • Minutes/meeting notes where the procedures have been reviewed during the year including the decisions made and any updates to the procedures.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines	Requirement No:	11-209
	Initiative:	Confidentiality and Data Protection Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

Organisations are responsible for the security and confidentiality of personal information they process. Processing may include the transfer of that information to countries outside of the UK, and where *person identifiable information* is transferred, organisations must comply with both the *Data Protection Act 1998* and the Department of Health guidelines.

Transfers Outside the UK

Introduction

1. The Data Protection Act 1998 implements into UK law Directive 95/46/EC of the *European Parliament* and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The aim is to harmonise data protection laws so that potential obstacles to cross-frontier flows of personal data between member states of the *European Union* (EU) are reduced and a high level of data protection within the EU is ensured.
2. Principle 8 of the Act governs transfers of personal information and requires that it is not transferred to countries outside of the European Economic Area unless that country has an adequate level of protection for the information and for the rights of individuals.

The European Economic Area

3. The European Economic Area (EEA) is made up of the EU member states plus the *European Free Trade Association* (EFTA) countries of Iceland, Liechtenstein and Norway. The current EU member states are in Table 1.

Table 1: The European Union Member States				
Austria	Belgium	Bulgaria	Cyprus	Czech Republic
Denmark	Estonia	Finland	France	Germany
Greece	Hungary	Ireland	Italy	Latvia
Lithuania	Luxembourg	Malta	Netherlands	Poland
Portugal	Romania	Slovakia	Slovenia	Spain

Sweden	United Kingdom			

4. Further details can be found on the EEA website.

An Adequate Level of Protection

5. The European Commission has the power to determine whether a third country (ie not an EU member state or an EFTA country) ensures an adequate level of protection for personal data by reason of its domestic law or the international commitments it has entered into.

6. The commission has so far recognised Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, the US Department of Commerce's 'Safe Harbor' Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.

7. Information on countries with an adequate level of protection and the US Safe Harbor agreements can be found within the European Commission decisions on the adequacy of the protection of personal data in third countries.

8. To ensure compliance, where an organisation discovers that it does transfer personal data to a country not listed in Table 1 above, it should check the website referred to in paragraph 7 to obtain up to date information about whether the country is deemed to have adequate protection.

9. If the transfer is to a third country not on the adequacy list, the organisation should put measures in place to ensure that there is an adequate level of protection when person identifiable information is transferred. This requires that contractual agreements are drawn up specifying the terms on which the information is transferred and the restrictions on its use for further purposes.

10. The organisation should assess all risks to the information and put protective measures in place to reduce any risks. Potential risk areas to be taken into account include:

    - what information is being transferred?
    - have the data subjects been informed?
    - to what country is the information being transferred?
    - what are the purposes of the transfer?
    - what data protection laws are in place in the overseas country?
    - is data protection appropriately covered in the contractual arrangements between the organisations?
    - is restriction on further use appropriately covered in the contractual arrangements between the organisations?
    - how is the information to be transferred?
    - what security measures are in place to protect the information during transfer?
    - what security measures are in place in the recipient organisation?

11. Further guidance is available from the Information Commissioner's Office detailed specialist guide, ‘The Eighth Data Protection Principle and International Transfers’ available from the Knowledge Base Resources.

Department of Health Guidelines

12. Organisations must also comply with the following guidelines issued by the Department of Health:

    - Person identifiable information must not be transferred outside of the UK unless appropriate assessment of risk has been undertaken (see paragraph 10) and mitigating controls put in place.
    - The organisation should review the flows of person identifiable information identified for **requirement 308 or requirement 322** , dependent on organisation-type, to understand whether information transferred to external organisations flows outside of the UK.
    - Information about overseas transfers of information must be included within the organisation’s Data Protection notification to the Information Commissioner and should ideally be included within the organisation’s Information Governance policy or equivalent document.
    - Decisions on whether to transfer person identifiable information must only be taken by a senior manager or senior care professional that has been authorised to take that decision.
    - Organisations will need to obtain an assurance statement from third parties that process the personal data of their service users or staff overseas. This assurance may be within the contract between the two organisations or within other terms of processing.

13. The Information Governance Policy website referenced in the **Knowledge Base Resources** should also be checked for any new guidelines.

Data Protection Act Principles

14. Whilst compliance with the eighth Principle is crucial, organisations must also consider all the other Data Protection Principles before making an overseas transfer of person identifiable data.

15. Of particular importance is the first Principle, which in most cases will require that individuals are properly informed about the transfer of their information to a country outside the UK.

Determining Whether the Requirement can be marked ‘Not Relevant’

16. Organisations acting purely as a data processor on behalf of a data controller should only be processing personal data in accordance with their contractual agreement with the data controller. Therefore, it is the data controller who is responsible for assessing their organisation against this requirement. Data processors must still comply with the other Data Protection principles.

17. Those organisations which act as data controllers, joint data controllers or data controllers in common must assess themselves against this requirement and ensure any overseas transfers of information are notified to the Information Commissioner.

18. Where an organisation has determined that it makes no transfers of personal information to non-UK countries this should be documented for audit purposes and the 'not relevant' attainment level option should be selected.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
Data Protection Act 1998	The Act that makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.	24/01/2013
Information Commissioner: The Eighth Data Protection Principle and International Data Transfers (PDF, 93 KB)	The Information Commissioner's recommended approach to assessing adequacy including consideration of the issue of contractual solutions, binding corporate rules and Safe Harbor.	24/01/2013
Information Commissioner: International Transfers of Personal Information (PDF, 122 KB)	This guidance provides practical advice to companies or other organisations who want to transfer personal information outside the EEA. It is not a complete statement of the relevant law, this is provided in the document 'the Eighth Data Protection Principle and International Data Transfers'.	24/01/2013
Information Commissioner: Data Protection Act 1998 - Legal Guidance (PDF, 255 KB)	This publication has been prepared by the Information Commissioner as a reference document for data controllers and their advisers. Where relevant, reference is made to some of the most important Statutory Instruments. This should assist in interpretation, as the secondary legislation introduces significant additional requirements.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Information Commissioner: Guidance Index	Here you can view a full index of the ICO's guidance for organisations.	24/01/2013
Information Commissioner: Contact Details	Frequently asked questions and help via phone, email and web form.	24/01/2013

European Commission: Decisions on the Adequacy of the Protection of Personal Data in Third Countries	EC international transfers home page with links to more detailed information on transfers of personal data from the EU/ EEA to third countries; binding corporate rules; commission decisions on the adequacy of the protection of personal data in third countries and frequently asked questions.	24/01/2013
Information Governance Web Pages	These pages contain policy, guidance, publications and links to materials on all aspects of information governance.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **The Caldicott Guardian in the NHS and Social Care** - a practitioner level module aimed at newly appointed Caldicott Guardians and those needing to know more about the role of the Caldicott Guardian.
- **Patient Confidentiality** - a foundation level module aimed at all NHS staff to gain an understanding of patient confidentiality and the role of the Caldicott Guardian in the NHS.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer tool** - comprising PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- Data Protection Act 1998
- DH guidance on overseas transfers 2009

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

NR	**Transfers of personal information have been reviewed and no overseas processing is carried out.**		❑
0	**There is insufficient evidence to attain Level 1.**		❑
1	**All transfers of personal information to countries outside the UK have been documented, reviewed and tested to determine compliance with the Data Protection Act 1998 and Department of Health (DH) guidelines.**		
	a	Responsibility has been assigned for reviewing information flows to identify overseas transfers. **Evidence Required:** • A named individual's job description, or a note or e-mail assigning responsibility or the terms of reference of a group.	❑
		Notes/other evidence:	
	b	All identified transfers of personal data to a country outside the United Kingdom have been documented and reviewed for compliance with the Data Protection Act and Department of Health guidelines. **Evidence Required:** • A documented report detailing all personal information flows to overseas locations and the result of risk assessments undertaken. This must be updated annually.	❑
		Notes/other evidence:	
2	**All transfers of personal data to countries outside of the UK fully comply with the Data Protection Act 1998 and DH guidelines. Where the review of overseas transfers reveals that appropriate contracts are not already in place for existing transfers, the organisation ensures that new contractual arrangements are signed.**		
	a	All transfers of personal data to countries outside of the UK fully comply with the Data Protection Act 1998 and DH guidelines. Where the review of overseas transfers reveals that appropriate contracts are not already in place for existing transfers, new contractual terms that appropriately cover data protection and place restrictions on further use must be negotiated with recipient organisations. **Evidence Required:** • Minutes/meeting note or document detailing senior management sign off of overseas transfers with a clear statement that all requirements have been met.	❑
		Notes/other evidence:	

	b	A review of current data processing and transfers has taken place during the current financial year and all changes to overseas transfers have been identified and new transfers assessed for compliance with the Data Protection Act 1998 and Department of Health guidelines. **Evidence Required:** • Refreshed evidence to satisfy 1(b) and minutes/meeting note confirming the current position and continued compliance	❑
		Notes/other evidence:	
3	**Transfers of personal data to non-UK countries are regularly reviewed to ensure they continue to fully comply with the Data Protection Act 1998 and DH guidelines.**		
	a	Transfers of personal data to non-UK countries are regularly reviewed to ensure continuing compliance. **Evidence Required:** • Documented details of the review of the transfers (eg checks that information is still being sent and received by the most secure method, and any decisions made to amend the transfer).	❑
		Notes/other evidence:	
	b	[Level 3 Maintenance - only required if Level 3 achieved in previous year] Policy and law change over time as do technological advances and it is important that the overseas transfer of personal data continues to comply with the law and central guidelines. **Evidence Required:** • Minutes/meeting notes where the transfers, recipients and contracts have been reviewed during the year including the decisions made and any updates.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements	Requirement No:	11-210
	Initiative:	Confidentiality and Data Protection Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

Organisations should ensure that when new processes, services, systems and other information assets are introduced that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements. For best effect, requirements to ensure information security, confidentiality and data protection and information quality should be identified and agreed prior to the design, development and/or implementation of a new process or system.

Impact and Risk Assessments

Introduction

1. All organisations experience change in one form or another. Rapidly changing technology has a major impact on processes and systems already in place, often requiring change simply to keep up to date and to enable the safe and secure processing of personal information.
2. It is vitally important that the impact of any proposed changes to the organisation's processes and/or *information assets* are assessed to ensure that the confidentiality, integrity and accessibility of personal information are maintained.
3. It should be recognised that changes to organisational processes and information assets may also be driven by service changes, for example:
    a. a new Consultant / senior practitioner or other caseload manager starting with the organisation;
    b. an existing Consultant / senior practitioner or other caseload manager leaving the organisation;
    c. a new service or clinic being commenced.

Responsibilities

4. The Information Governance forum (or equivalent group that considers information governance compliance issues) should be consulted during the design phase of any new service, process or information asset so that they can decide if a privacy impact assessment is required for a particular project or plan.
5. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by a senior person that leads

on information risk (eg in the NHS, the *Senior Information Risk Owner* - SIRO and *Information Asset Owners* - IAOs). NHS organisations should be aware that DSCN 18/2009 (available in the **Knowledge Base Resources**) advises that whenever any new IT system is introduced, a responsible person should be charged with making sure that it is clinically safe. That responsibility would include aspects of data quality, ie does the new system produce data that can be relied on for clinical decision-making?

6. Development of *IG security accreditation documentation* should be carried out by those staff with the best knowledge of a planned, new or existing information asset, its intended purposes and its operating environments. This development should be overseen by the senior person that leads on information risk.

7. All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to seek approval from the group that considers information governance compliance issues.

Compliance with Information Quality, Confidentiality and Data Protection Requirements

8. Compliance with confidentiality and data protection must be taken into account and there must also be a comprehensive consideration of potential impacts on information quality at the design phase of any new process or information asset. Some of the considerations that should be taken into account are whether a new process or information asset will:

    - affect the quality of personal information already collected;
    - allow personal information to be checked for relevancy, accuracy and validity;
    - incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required;
    - have an adequate level of security to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage;
    - enable data retrieval to support business continuity in the event of emergencies or disasters;
    - enable the timely location and retrieval of personal information to meet subject access requests;
    - alter the way in which the organisation records in or monitors and reports information from a key operational system.

9. The *Information Commissioner's Office* has developed a Privacy Impact Assessment (PIA) handbook that will assist organisations to ensure that privacy concerns and safeguards are addressed and built in as a project or plan develops. The handbook contains a screening tool to enable a decision on whether a PIA is needed, and if so, whether the project requires a Full-Scale PIA or a Small-Scale PIA (both are defined in the handbook). The handbook is available from the **Knowledge Base Resources**.

Compliance with Information Security Requirements

10. Information security related aspects of IG including any risk to the integrity of information should be identified, considered and necessary actions integrated and documented in the overall project or plan for the new process or information asset.

11. An information security risk analysis should be carried out at an early stage of each project to identify requirements for design and risk mitigation purposes. The security controls should address all developmental and operational aspects of the asset and become an integral aspect of the project. The Information Security Manager (or equivalent) should be involved as part of the project team throughout to ensure the selected security controls are identified and implemented properly and tested satisfactorily.

12. Appropriate IG security accreditation documentation must be developed and maintained for all security controls applied to a particular information asset including assessments and assurance reviews of those controls, to assess their effectiveness in mitigating identified risks to that information asset.

Information Assets: IG Security Accreditation

13. Although the definition of an information asset incorporates ‘softer’ aspects such as the skills or specialist knowledge of staff members, in the majority of cases IG security accreditation would have most relevance to the ‘hardware’ and ‘software’ components of an information asset, including their configuration settings.

14. Accreditation documentation will provide those leading on information risk (eg SIRO and IAO or equivalent) with assurance that information security has been properly considered and addressed within the design, development, implementation, operation and decommissioning stages of an asset’s lifecycle.

15. Accreditation will normally be achieved in stages aligned to the asset’s project feasibility, design, development and implementation stages and should be routinely reviewed and extended or refined throughout its operating lifetime. Further detail on asset accreditation is contained in the NHS Information Risk Management: Good Practice Guideline, available from the **Knowledge Base Resources**. Other aspects to be considered are discussed below.

Project Management – PRINCE 2

16. The NHS IM&T ‘Good Practice Guidance for NHS Board Members’ refers to Projects in Controlled Environments (PRINCE 2). An approved methodology such as PRINCE or similar tool provides a structured and logical approach to conducting projects and should be utilised when developing new information assets.

17. Though not a statutory requirement, the following are the main stages of development for IM&T projects that the Information Governance lead or group (or equivalent) should ensure are reflected in project plans and controls:

    - requirements analysis;
    - functional specification;
    - system architecture and design;
    - creation or selection of software;
    - testing;

- assuring fulfilment of project objectives;
- assuring quality;
- acceptance and implementation;
- operation and maintenance.

18. Existing provisions for project management should be reviewed to determine whether they are in accordance with the stages above.

Separation of Development, Test and Operation Facilities

19. Processes or information assets in development or under test can potentially cause problems to operational systems, so should be separated until approved for introduction as operational systems. The final test, that of a new process or asset being run as an integral part of the organisation's operations, should be carefully monitored as some problems only become apparent at this last stage.

20. The IAO (or equivalent) should ensure that documented procedures are in place governing the transfer of components from development to operational environments.

21. Development software and test data should be run on different systems or domains until all tests are successfully completed. Operational data, including person identifiable data, must not be used for test purposes as this may endanger its integrity and reliability and/or may cause an unforeseen security event.

22. Access to development tools and system utilities should be restricted to relevant authorised personnel only and must not be accessible from operational systems.

23. Testing environments should attempt to emulate the operational environment as far as possible. Preferably, a test domain will include replications of all the operational systems it will interface with. This will increase the likelihood that conflicts between the new asset/process and other operational systems will be identified during testing. For this to be valid, it is important that updates, patches, etc for operational systems are also replicated in the test environment.

24. Separate user IDs should be established for use on test systems.

25. Test systems should be subject to the same access and security controls as operational systems. This provides protection for the systems and allows staff an opportunity to experience and practice operational procedures. Test data should be backed up to ensure the integrity of the test system.

Capacity Planning

26. The capacity of the existing infrastructure to cope with the introduction of new or amended processes or assets should be considered as part of the implementation planning process. Bandwidth, storage space, technical and helpdesk support, other staffing, maintenance and replacement costs and implications should all be taken into consideration.

27. Additional physical resources such as accommodation, furniture, paper supplies, training materials and material storage cabinets need to be considered. Increased deliveries of supplies will need to be considered, both at central delivery and local areas.

Acceptance

28. The following criteria should be included for new processes and information assets:

    a. error recovery and restart procedures;

    b. preparation and testing of routine operating procedures to defined standards;

    c. an agreed set of security controls;

    d. training in the use of the information asset or process for user and technical/ helpdesk support;

    e. user involvement at all stages of asset or process development to ensure the new way of working is as intuitive as possible.

Agreed Set of Security Controls

29. These should include:

    a. effective manual fallback procedures;

    b. business continuity and disaster recovery arrangements;

    c. evidence (through testing, calculations and validation of data) that the new assets or processes will not adversely affect existing operational systems.

Guidance for Staff

30. Documented operating procedures should be made available for all users of information assets, as part of user training. It is essential that these procedures are kept up to date, to reflect any implications of changes to software/hardware or working methods. System administrators and technical support personnel will also need access to more detailed operating procedures to carry out their roles. The operating procedures should become part of the information asset register (see **requirement 307** or **316** dependent on organisation-type) and become subject to regular review. Typically, the procedures should include:

    a. information processing and handling instructions;

    b. information backup procedures (see **requirement 309**);

    c. job scheduling requirements, including interdependencies with other information assets;

    d. instructions for handling errors;

    e. restrictions on access to and use of system utilities;

    f. support contacts for operational or technical difficulties;

    g. instructions for handling output and media, including the disposal of confidential waste and failed jobs;

    h. system restart and recovery;

    i. the management of audit and log data (see also **requirement 305**).

Change Management

31. System software, hardware and operating procedures are subject to regular change. It is essential that any changes are subject to a strict change management regime,

to ensure that all changes are controlled and approved. These change procedures are normally achieved under the direction and authority of the asset owner (for NHS Trusts, the IAO) or their responsible *Information Asset Administrator* (or equivalent). Failure to do this can result in patching deficiency and unforeseen system faults or failures. Formal documented change management procedures should be put in place, which will typically include the following:

a. change management structures, responsibilities and approval processes;

b. identification and recording of changes;

c. proposed change impact analysis;

d. communication plan for proposed changes;

e. fallback procedures in case of unforeseen errors/problems following change.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
Confidentiality NHS Code of Practice 2003	The Code is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their information.	24/01/2013
HSCIC: Good Practice Guidelines - Application Security	This guide covers various general user applications and their security.	24/01/2013
DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013

DH: NHS IG - Information Risk Management - Good Practice Guide 2009	This guidance is aimed at those responsible for managing information risk within NHS organisations. It reflects government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures in Government'. This GPG also includes guidance on the need for Forensic Readiness Policy and local implementation.	24/01/2013
DH: Records Management NHS Code of Practice 2008	The Code is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The guidance applies to all NHS records and contains details of the recommended minimum retention period for each record type.	24/01/2013
Information Commissioner: Privacy Impact Assessment Handbook	The ICO handbook is designed to be a practical and comprehensive guide, aimed at organisations who are developing projects that might have implications for people's privacy. It will help organisations assess and identify any privacy concerns (a Privacy Impact Assessment) and address them at an early stage, rather than leaving the solutions to bolt on as an expensive afterthought.	24/01/2013
BS ISO/IEC 27000 Series of Information Security Standards	Note that only NHS Information Governance Toolkit (IGT) administrators may download a copy of the standards for use by their organisation. The administrator must be logged on to download these standards.	24/01/2013
BS ISO/IEC 20000-2:2005 Information Technology Service Management Code of Practice	The Code offers assistance to service providers planning service improvements or to be audited against BS ISO/IEC 20000-1:2005 and can be purchased from the BSI website.	24/01/2013
Data Protection Act 1998	The Act that makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.	24/01/2013

HSCIC: Good Practice Guidelines in Information Governance - Information Security	The Good Practice Guidelines (GPG) are a series of informational documents which provide best practice advice in technology specific areas of Information Security.	24/01/2013
DSCN 18/2009 Patient Safety Risk Management System - Deployment and Use of Health Software	This standard specifies the risk management processes required to minimise risks to patient safety in respect to the deployment and use of software products either as new systems within a health organisation or as changes to an existing systems environment.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Walton Centre: Change Control Standard (PDF, 141 KB)	An operational change control process covering change initiation of change, control of change, record keeping, and decision making for all aspects of change on the Trusts information systems on computer.	24/01/2013
IT Operations: Operational Change Control (PDF, 92 KB)	The aim of this document is to put in place procedures that minimise the risk of damage to an organisation's information systems, data and business that may come from changes to its computer systems.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Cabinet Office: Best Management Practice Portfolio	Best Management Practice products present flexible, practical and effective guidance, drawn from a range of the most successful global business experiences. Distilled to its essential elements, the guidance can then be applied to every sort of business and organisation.	24/01/2013
ITIL: The IT Infrastructure Library	The ITIL series of publications is designed to provide advice on how to prepare and deal with IT related management problems. The publications are available to purchase from the TSO online bookshop.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **The Caldicott Guardian in the NHS and Social Care** - a practitioner level module aimed at newly appointed Caldicott Guardians and those needing to know more about the role of the Caldicott Guardian.
- **Patient Confidentiality** - a foundation level module aimed at all NHS staff to gain an understanding of patient confidentiality and the role of the Caldicott Guardian in the NHS.
- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of Information risk management. Staff whose roles involve the handling of personal data will benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.
- **NHS Information Risk Management** - a foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.
- **NHS Information Risk Management for SIROs and IAOs** - an introductory module that describes key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties. SIROs should also review the IRM Foundation module.
- **Records Management and the NHS Code of Practice** - a foundation level module designed to provide practical information to enable understanding of the importance of good records management.
- **Records Management in the NHS** - a practitioner level module designed to provide practical information and steps for the operational running, policy creation and strategy in relation to record management.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- Caldicott: Report on the Review of Patient Identifiable Information 1997
- Data Protection Act 1998
- Information Security NHS Code of Practice 2007

- ISO/IEC27002 controls (revised 2005) ref 10.1.1 - 4, 10.3 & 12.1

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**There is a documented procedure and structured approach for ensuring that new or proposed changes to organisational processes or information assets are identified and flagged with an appropriate information governance group or equivalent and that information security, confidentiality and data protection, and information quality requirements are defined at an early stage of the project cycle.**		
	a	Responsibility for documenting a procedure to ensure that new or proposed changes to organisational processes or information assets are identified has been assigned to an individual or group. **Evidence Required:** • A named individual's job description, or a note or e-mail assigning responsibility or the terms of reference of a group (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	b	There is a documented procedure for the identification and assessment of new processes and information assets that might impact on information security, confidentiality and data protection, and information quality that sets out a range of responsibilities for those involved in making decisions about whether to permit implementation of a new process or information asset. The type of roles that would typically be involved would be the senior people that lead on confidentiality (eg Caldicott Guardian), information risk (eg SIRO, IAO), information security officers, IG leads, etc. **Evidence Required:** • A written document detailing a named group or job role(s) that decides whether a privacy impact assessment is required, considers any impact on information quality, reviews existing security procedures and identifies any new security procedures that may be required (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	c	The procedure also sets out a structured approach for appropriate IG security accreditation documentation, procedures and controls to ensure new information assets are developed and introduced in a secure manner. **Evidence Required:** • A documented project management approach to new and proposed changes to organisational information assets, or documented procedures and controls (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	

2	**All staff members who may be responsible for introducing changes to processes or information assets have been effectively informed about the requirement to seek approval from the appropriate group. All new implementations follow the documented procedure. Where the proposed new process or information asset is likely to involve a new use or significantly change the way in which personal data is handled, an appropriate privacy impact assessment is always carried.**		
	a	All staff members that are likely to introduce new information processes or information assets are effectively informed about the requirement to obtain approval from the IG forum (or equivalent) at the proposal stage of the new process or information asset. Staff might be informed through team meetings, awareness sessions, or staff briefings. **Evidence Required:** • Minutes/meeting papers, or notes of team meetings, or staff briefing materials or awareness sessions materials (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	b	All implementations of new processes and information assets follow the documented procedure, including adhering to the structured project management process for the implementation of new information assets. Information governance requirements are well defined and selected, and risks and issues are identified early and addressed routinely. An appropriate privacy impact assessment is carried out whenever a new process or information asset is likely to involve a new use or significantly change the way in which personal data is handled. Robust change control processes are applied. **Evidence Required:** • Project documentation, formal risk analysis of information governance considerations identified prior to implementation, and where necessary privacy impact assessment documentation (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate). • Change control documents (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
3	**Compliance with the guidance is monitored by reviewing any new processes or information assets that have been introduced. Project assurance processes are in place and the results are fed through project boards or similar groups. Remedial or improvement action is documented and taken where appropriate.**		
	a	Specific project IG assurance processes are in place to review the new processes and information assets. Results are appropriately fed through to appropriate personnel/ groups (eg information risk leads, IG group, project boards, etc). Where a need for improvement is identified, this is documented within plans and appropriate action taken. **Evidence Required:** • Minutes/meeting notes where the new processes and information assets have been reviewed during the year including the decisions made, and where necessary, action taken to make improvements or any updates to the new processes or information assets.	❑
		Notes/other evidence:	

	b	Providing staff with written materials or briefings does not provide sufficient assurance that the procedure has been understood and that the advice and approval of the IG group is obtained before new processes or information assets that might impact on information security, confidentiality and data protection, and information quality are introduced. Therefore, compliance spot checks and routine monitoring are conducted. **Evidence Required:** • Completed monitoring forms, a report on the outcome of staff compliance checks or a review report of requests for approval compared with the new processes or information assets introduced.	❑
		Notes/other evidence:	
	c	[Level 3 Maintenance - only required if Level 3 achieved in previous year] Policy and law change over time and it is important that the content of the documented procedure and structured approach is regularly reviewed and aligned with the latest central guidelines. **Evidence Required:** • Minutes/meeting notes where the procedure and approach has been reviewed during the year including the decisions made and any updates to the procedure and approach.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

All transfers of personal and sensitive information are conducted in a secure and confidential manner	Requirement No:	11-211
	Initiative:	Confidentiality and Data Protection Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

There is a need to ensure that all transfers of personal and sensitive information (correspondence, faxes, email, telephone messages, transfer of patient records and other communications containing personal or sensitive information) are conducted in a secure and confidential manner. This is to ensure that information is not disclosed inappropriately, either by accident or design, whilst it is being transferred or communicated to, within or outside of the organisation.

Transfers of Personal and Sensitive Information

Introduction

1. Transfers of personal and sensitive information within and between organisations should be controlled, and should be compliant with any relevant legislation, for example the *Data Protection Act 1998*.
2. The loss of personal information will result in adverse incident reports which will not only affect the reputation of the organisation but, in the case of disclosing personal information intentionally or recklessly, is also a criminal offence. With effect from April 2010 fines of up to £500,000 may be imposed by the *Information Commissioner's Office* on organisations that do not take reasonable steps to avoid the most serious breaches of the Data Protection Act.

Defining Personal and Sensitive Information

3. **Personal Information**. This 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 items 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.
4. **Sensitive Information**. This can be broadly defined as that which if lost or compromised could affect individuals, organisations or the wider community. This is wider than, but includes, information defined as sensitive under the Data Protection Act 1998, eg an individual's bank account details are likely to be deemed 'sensitive', as are financial and security information about an organisation.

Movement of Personal and Sensitive Information

5. Information is commonly moved around and between organisations, whether in paper health records, in electronic form or on other media. Where this information is personal or sensitive information it must be transferred with appropriate regard to its security and confidentiality. It is also essential that the media are protected from unauthorised access and environmental damage at all stages of the move. External exchanges should be carried out on the basis of agreements between exchanging organisations.

6. Procedures and standards to protect information and media (paper, electronic storage media, photos, X-rays, etc) in transit should be established. The business and security implications associated with transferring information electronically, eg by email should be considered.

7. There must also be procedures in place to ensure all personal and sensitive information relating to patients/service users is received to a secure and protected point. These secure points, also referred to as '*safe havens*' should be in place wherever the information is received, including transcribing of phone messages, fax in-trays, electronic mailboxes, pigeon holes and in-trays for paper information etc.

Appropriate Transfer Methods

8. Guidelines on appropriate transfer and protection measures are provided below under the following headings:

    - surface mail and couriers;
    - email;
    - non-computerised information.

Surface Mail and Couriers

9. Secure post should be used for the transmission of personal information between organisations and the addressee requested to acknowledge receipt of the information. Secure packaging, that will clearly show if it has been tampered with, should be used.

10. If personal information is regularly received by post, it is essential that physical security measures, such as, key coded or swipe card entry, or lockable doors/ cabinets are in place to protect information in the post-room, post collection point or similar.

11. Internal post containing personal information transported within and between an organisation's sites should be carried in lockable satchels to protect it from loss or accidental viewing.

12. *Encryption*: Encrypted electronic media transported between sites or organisations should be properly packaged and clearly labelled to ensure they are handled correctly and not corrupted by magnetic fields.

13. In accordance with NHS Chief Executive - David Nicholson's letter of 15th January 2009, unencrypted transfers of *patient identifiable information* by courier or post should be suspended unless they are essential for patient care.

14. Where a decision is made to continue to transfer unencrypted information, this must be specifically signed off by a senior member of staff and, where necessary, notified

to the *commissioning organisation* with a description of how the information will be protected.

15. Where a decision is made to suspend a data transfer, a senior member of staff must be made aware and, where necessary, the commissioning organisation should be informed of any plan as to how the transfers are to be replaced or made secure. This applies to all patient identifiable data.

16. As regards General Practice, the Department of Health has discussed these matters with the Royal College of General Practitioners and the General Practitioners' Committee to ensure that good practice is clarified and disseminated.

Email

17. Email is not a secure system. All staff using email should be made aware of this during their induction training and during any training provided for use of the email system. Therefore, patient identifiable and other sensitive information should not be sent by email unless it has been encrypted to standards approved by the NHS.

18. *NHSmail* accounts are encrypted to NHS-approved standards and may be used for sending patient identifiable information to recipients that also have an NHSmail account. There is still a need to be certain about the identity of the recipient. It is imperative that all users are aware that the information is encrypted only between NHSmail accounts.

19. Emails containing patient identifiable information should not be sent to non-NHSmail accounts, as they are not encrypted, even if sent from an NHSmail account. All users must be fully trained in the use of email and NHSmail accounts.

20. Emails containing patient identifiable information must be stored appropriately on receipt, eg incorporated within the individual's record, and deleted from the email system when no longer needed.

21. Email attachments are one of the most common methods for transmitting viruses. All users should be informed of the dangers posed by opening attachments, especially those they were not expecting. Up-to-date *anti-virus* software should be used to check attachments and lock particular file types.

Non-Computerised Information

22. A fax machine used to receive person identifiable or sensitive information must be located in a secure environment. Additionally, the fax should be removed from the machine on receipt and appropriately dealt with and safely stored. Where appropriate, the sender should be contacted to confirm receipt.

23. Patient *digital* images (still or moving) are being used more often. If digital/video images are part of the patient record, they must be transferred and retained in accordance with the *Caldicott Principles* and stored securely. Audio recordings of patients should be treated in a similar manner to digital images.

24. Recorded telephone messages may contain sensitive personal information, for example, the names and addresses of applicants phoning for a job. Therefore, they need to be properly secured so that only those entitled to listen to the message may do so. Telephone and other messages taken in another's absence should be recorded by a dedicated method that is kept secure and confidential.

The Caldicott Principles

25. The Principles were devised by the *Caldicott Committee*, which reported in 1997 following a review of patient-identifiable information. They represent best practice for using and sharing identifiable personal information and should be applied whenever a transfer of personal information is being considered.

Table 1: The Caldicott Principles:
• Principle 1: Justify the purpose for using the 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

General Retention / Appropriate Storage Issues

26. Organisations should ensure that when personal or sensitive information is received it is stored securely with access only by those with a legitimate right to the information. The type of storage that is appropriate will depend on the media on which the information is received.

27. To comply with the provisions of the Data Protection Act 1998, personal information must not be retained for longer than is necessary to carry out the purpose for which the information was provided.

Procedures and Guidance for Staff

28. There should be procedures for staff covering appropriate methods of transfer of personal and sensitive information within or from the organisation and also procedures for receipt of information in the organisation – the 'safe haven' procedures. Before transferring information, staff should be directed to obtain answers to the following questions based on the Caldicott Principles:

    - is there a valid need to use/disclose confidential information?
    - is it necessary to use confidential information?
    - has the minimum possible confidential information been used?
    - do the proposed recipients need to know all of the confidential information?
    - have all staff members been informed of their responsibilities for protecting confidential information?
    - is the use of confidential information lawful?

29. All areas from which correspondence, faxes, email, telephone messages, transfer of patient records and other communications containing personal information may be sent should be identified, and procedures developed to ensure security and confidentiality are maintained. The types of issues the procedures should address are:

    - how much information can be given, eg on the phone;

- where and how incoming messages are recorded, eg a message book;
- when a particular type of mail route may be used, eg email;
- when a courier should be used;
- discussion of patients in public.

This is by no means an exhaustive list, but may be used as a starting point, in considering the procedures and processes required.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
Care Quality Commission: Guidance about compliance with the Essential Standards	The essential standards of quality and safety are central to the Care Quality Commission's (CQC) work in regulating health and adult social care. Each of the standards has an associated outcome that CQC expects all people who use services to experience as a result of the care they receive. Outcome 21: Records, sets out the requirement for people's personal records, including medical records, to be accurate and kept safely and confidentially.	24/01/2013
Confidentiality NHS Code of Practice 2003	The Code is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their information.	24/01/2013
The NHS Care Record Guarantee for England	The Guarantee sets out the rules that govern how patient information is used by all organisations providing care for or on behalf of the NHS and what control the patient can have over this.	24/01/2013
DH: NHS IG - Good Practice Guide for the Transfer of Batched Person Identifiable Data	Good Practice Guidelines for the transfer of batched person identifiable data by means of portable electronic media. These equally apply to back ups and data destruction.	24/01/2013
DH: NHS IG - Guidelines on Use of Encryption to Protect Person Identifiable and Sensitive Information 2008	Encryption guidance published by the Department of Health Information Governance Policy team.	24/01/2013

DH: NHS IG - Short Message Service & Texting (PDF, 48 KB)	IG Policy team guidance that provides NHS organisations with a general awareness of the associated risks of Short Message Service (SMS) and texting that may potentially affect the effectiveness of local services, April 2010.	24/01/2013
General Medical Council: Confidentiality 2009	Confidentiality (2009) sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. Supplementary guidance explaining how these principles apply in situations doctors often encounter or find hard to deal with is also available.	24/01/2013
British Medical Association: Confidentiality and Disclosure of Health Information Tool Kit	The purpose of this tool kit is not to provide definitive answers for every confidentiality and disclosure situation but to identify the key factors which need to be taken into account when such decisions are made.	24/01/2013
Joint IT Committee: The Good Practice Guidelines for GP electronic patient records Version 4 (2011) (PDF, 1732 KB)	The new Good Practice Guidelines for GP electronic patient records v4 (GPGv4 2011) will act as a reference source of information for all those involved in developing, deploying and using general practice IT systems.	24/01/2013
HSCIC: Good Practice Guidelines - Application Security	This guide covers various general user applications and their security.	24/01/2013
HM Government: Information Sharing Guidance (PDF, 1111 KB)	Cross Government guidance that aims to provide practitioners with clear guidance about when and how they can share information legally and professionally about the individual they are in contact with.	24/01/2013
Information Mapping Tool Guidance	Supporting guidance explaining the principles which should be considered for the mapping exercise. Access to this Tool is only available when logged into the Information Governance Toolkit (IGT).	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
IG Resource Pack	These useful resources comprise staff awareness leaflets, exemplars, templates and model documents. Practices should scroll down the page for GP requirement specific resources.	24/01/2013
Surrey HIS: Data Protection Leaflet - Best Practice Guidelines (PDF, 272 KB)	Leaflet for staff produced by Surrey Health Community in 2006.	24/01/2013
Bite-sized Good Practice Guide: Safe Computing (DOC, 347 KB)	IG Policy team leaflet on good practice in safe computing.	24/01/2013
Bite-sized Good Practice Guide: Internet and Email (DOC, 393 KB)	IG Policy team leaflet on good practice in using the internet and email.	24/01/2013
General Practice template: Staff Declaration Form.doc (DOC, 57 KB)	A form for staff to sign to confirm that they have received information and guidelines regarding information governance in the practice.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
NHSmail - Public-Facing Site	Information and case studies about the benefits of using the secure email and directory service available to all NHS staff.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **Secure Transfers of Personal Data** - a foundation level module that informs learners how to protect sensitive data from unauthorised access and accidental loss, damage or destruction during transfer and how to dispose of sensitive data when it is no longer needed.
- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of information risk management. Staff whose roles involve the handling of personal data will

benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.

- **Information Security Guidelines** - an introductory module on keeping information secure in and out of the workplace.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- Caldicott: Report on the Review of Patient Identifiable Information 1997
- Data Protection Act 1998
- Health Service Circular 1999/012 Caldicott Guardians
- Protecting and Using Patient Information: A Manual for Caldicott Guardians 1999
- Confidentiality: NHS Code of Practice 2003

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**All areas from which personal and sensitive information is transferred and received have been identified. A procedure is in place to ensure security and confidentiality is maintained.**		
	a	All areas from which personal and sensitive information is sent or received have been identified. **Evidence Required:** • List of the relevant areas.	❑
		Notes/other evidence:	
	b	There is a documented procedure for the secure transfer and receipt of personal and sensitive information. **Evidence Required:** • A document, staff handbook, or leaflet.	❑
		Notes/other evidence:	
	c	The procedure has been approved by senior management. **Evidence Required:** • Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriately senior manager.	❑
		Notes/other evidence:	
2	**All staff members have been informed about the procedure on secure transfer and receipt of personal and sensitive information and of the need to comply with it.**		
	a	The procedure has been made accessible to staff in an appropriate location. **Evidence Required:** • Inclusion in a staff handbook or by publishing it on the Intranet, or staff may be provided with their own copy of the procedure. In the latter case there may be a list of staff signatures confirming receipt of the procedure or the evidence may be a description of the publication process or minutes of the meeting where this was decided.	❑
		Notes/other evidence:	
	b	All staff members have been informed of the procedure and in particular of their own responsibilities for compliance. **Evidence Required:** • Minutes/notes of team meetings, or briefing materials from awareness sessions.	❑
		Notes/other evidence:	

	c	All new staff, temporary and contract staff members are made aware of the procedure and in particular of their own responsibilities for compliance. **Evidence Required:** • Staff induction materials and in staff signature lists - that they have read and understand why they must comply with the guidance.	❑
		Notes/other evidence:	
3	**Staff compliance with the procedure is monitored. The procedure is reviewed and evaluated on at least an annual basis.**		
	a	Providing staff with guidance materials and briefings does not provide sufficient assurance that the guidance has been understood and is being followed, therefore compliance spot checks and routine monitoring are conducted. **Evidence Required:** • Completed monitoring forms, or a report on the outcome of staff compliance checks.	❑
		Notes/other evidence:	
	b	[Level 3 Maintenance - only required if Level 3 achieved in previous year] Policy and law change over time and it is important that the content of procedure is regularly reviewed to ensure it continues to provide secure and confidential methods for transferring and receiving patient information. **Evidence Required:** • Minutes/meeting notes where the procedure has been reviewed during the year including the decisions made and any updates to the procedure.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems	Requirement No:	11-305
	Initiative:	Information Security Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

Organisations should control access to *Information Assets* and systems. This may be achieved by ensuring that system functionality is configured to support user access controls and by further ensuring that formal procedures are in place to control the allocation of access rights to local information systems and services. These procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given to managing access rights which allow support staff to override system controls.

Access Controls and Controls Functionality

Introduction

1. The guidance provided below reflects general good practice for information system specification, design, and proper usage. Organisations should apply this guidance when considering or reviewing access and control functional requirements for existing and new systems, and the individuals and groups requiring access. In the case of national systems, access control requirements include the use of approved user NHS Smartcards.
2. Access to information assets, information processing facilities, and business processes should be controlled on the basis of business need and security policy requirements. Access control rules should take account of both local and national policies, where these exist, for information dissemination and authorisation.
3. This requirement is scoped to include all operating systems (eg Linux or Windows variants etc), application and information systems (eg patient / service user administration system, Microsoft Excel).

Information Assets: Computer-Based Information Systems Access Controls

4. This requirement is concerned with access controls for computer-based information assets. Paper-based information systems controls are explained in more detail within the Corporate Information Assurance requirements and, where applicable, the Clinical Information Assurance requirements within the IG Toolkit. The individual responsible for the protection of an Information Asset (in NHS Trusts this will be the *Information Asset Owner* (IAO)) and the Information Security lead should liaise with

those responsible for Records Management requirements to ensure controls for paper records meet the requirements of information security standards.

Information Assets: Access Controls and Related Functionality

System Level Security Policy / Access Control Policy

5. Each key information asset should have IG accreditation documentation that includes a system level security policy that contains rules regarding its access control. The system level security policy should be approved by the Information Asset Owner (or individual with equivalent responsibilities), and Information Governance Board (or equivalent), be available to all users who are granted access to the system and should be reviewed on a regular basis. A typical system level security policy should take account of the following:

    a. The System Security Requirements. A risk assessment for the system will help determine the security requirements. For example, the level and type of access controls, location of hardware associated with the system, type of data held, etc.

    b. Identification of all information related to the system, and possible risks to the information. For example, a system holding patient data. A risk analysis will point to risks of unauthorised access, input of inaccurate data, corruption of data, loss of processing facilities, etc.

    c. Rules for information dissemination and authorisation eg dissemination based on a need to know basis and authorisation to data based on granular user profiles.

    d. Consistency between the access control and any information classification policies of different systems and networks. This applies where an information classification scheme has been implemented within the organisation.

    e. Relevant legislation and any contractual obligations regarding protection of access to data or services. Reference should be made to legislation such as the *Data Protection Act 1998*, *Freedom of Information Act 2000*, *Computer Misuse Act 1990*, etc. Any national NHS or other relevant guidelines should also be acknowledged.

    f. Standard user access profiles for common job roles in the organisation. This relates to granularity of access. In practice, system user profiles should be kept to a minimum, based on business needs. For small departmental systems, this can mean administrator; user with ability to read, create, amend, delete, copy and print files; user with ability to read only, etc. However, systems with a wide variety of users will require significant thought in devising and reviewing access profiles.

    g. Management of access rights in a distributed and networked environment which recognises all types of connections available. The policy should take account of the ways in which users can get access to the system eg local workstation only, any networked workstation, remote access, wireless, etc; and ensure secure access procedures for those applicable are put in place.

    h. Segregation of access control roles. The Information Asset Owner (or individual with equivalent responsibilities) should ensure that written procedures are produced that cover access requests, authorisation and

administration. The procedures should ensure that no single member of staff is able to authorise all access.

i. Requirements for formal authorisation of access requests. Information Asset Owners should ensure that a written procedure exists detailing how to apply for access and how to process applications.

j. Requirements for periodic review of access controls. The review should ensure that user accounts remain appropriate. For example, is the account still used, has the user changed role, do changes to the system call for a new assessment of role-based access, etc

k. Removal of access rights. Documented procedures should exist that include the criteria for removal of access rights, who authorises removal and when removals are permitted, and for audits of removals.

l. Forensic readiness policy. Organisations should ensure that systems are capable of providing admissible digital evidence, if required by an investigation or legal proceedings. View an example Forensic Readiness Policy.

6. It should be remembered that the policy document does not need to include specific details of all these criteria. Full procedures should then be documented to support the policy.

Secure Logon Procedures

7. All computer systems should have a logon authentication procedure that includes at least a unique user ID and password (some systems may potentially require additional authentication, such as user Smartcard). A risk assessment should help determine what level of authentication is required. The following features should be considered:

a. System/application identifiers should not be displayed until the logon procedure has been successfully completed.

b. A ‘pop-up’ window or prime-screen acceptable use warning that the workstation should only be accessed by authorised users. This will not stop determined unauthorised users, however, it does show that the organisation has demonstrated that the system is not freely available and that unauthorised use may contravene the Computer Misuse Act 1990.

c. Do not indicate which part of the logon information is incorrect eg if a user makes an error. This prevents unauthorised users identifying patterns when attempting to gain access to systems.

d. Limit the number of unsuccessful consecutive logon attempts. Many systems allow three unsuccessful attempts before locking users out. A pop-up window then advises the user to contact a helpdesk to have the password reset. The system can also be set to record unsuccessful logons (useful to identify frequency of errors and to alert of a possible hacking attempt).

e. Limit the maximum time allowed for logon.

f. The system should record the date and time of successful logons. Logs may be used during investigations. The log is therefore a valuable source of

evidence and should be linked to a workstation identity (the Media Access Control (MAC) address will be needed to do this).

g. The password being entered should not be displayed in clear text. Most systems show a number of asterisk characters and some systems nothing at all in the password field.

h. Passwords should not be transmitted in clear text over the network. Passwords should be encrypted through, for example, a RSA or hashing algorithm, for transmission over networks.

i. Systems should enforce password changes after a specified period of time.

Identifying and Authenticating Users

8. In order to facilitate and operate effective access control and audit functions it should be possible to uniquely identify all users of an information asset. This function may potentially be achieved by unique username and password combination or, in systems containing sensitive information, secondary smart token technology and biometrics.

9. Group IDs prevent successful audits being carried out that trace actions to an individual and should therefore only be used if absolutely necessary and in locally approved circumstances . Where group IDs are used a record of those users with access to the group ID should be held.

Password Management System

10. Password management systems are used to establish rules concerning the use of passwords in the system. The system owner should establish the rules, which will then be implemented by the system administrator. The following criteria should be considered:

    a. Is it absolutely necessary to use group passwords on the system? In all but exceptional circumstances, all users will be identified as individuals (including system administrators) when they log on.

    b. Do users have to change their initial password (issued by the system administrator) following their first logon? Users should be encouraged to set their own password, as it will usually be based on something they can remember.

    c. Are web browsers configured to prevent the recording of website passwords when logging in to web based applications? Recording of website passwords renders the password ineffective as a security measure. Passwords are therefore best if manually entered by the user at each login to be effective.

    d. Does the system log user passwords and prevent re-use? Repetitive re-use of passwords weakens the effectiveness of the password and should be avoided.

    e. Can users change their own passwords when they wish? This function increases security as users can change passwords, if they feel their current one has been compromised.

    f. Are complex passwords required? Simple passwords (less than 6 characters, number or letter only, repeated use) pose a threat to the system.

Alphanumeric passwords of 6 characters or more should be considered for any system. More details are available in a User Guide to Passwords.

g. Are periodic password changes enforced? A maximum period of three months between enforced changes is the norm for most systems.

h. Are passwords displayed on the screen when being entered? Displayed passwords can obviously be seen by others and pose a security threat. Most systems now display only asterisks when characters are entered and some systems do not display anything. One of these latter rules should be implemented.

i. Are passwords stored separately from application system data? Crackers normally search application sub-folders to locate password files. Therefore, every care should be taken to store passwords in protected network folders. Advice on protecting password files and illustrations of vulnerabilities in named application password file storage is on the CERT website.

j. Are passwords stored and transmitted in encrypted or hashed form? All passwords should be stored or transmitted using encryption or hashed.

11. The following control measures will apply.

Use of System Utilities

12. Some systems may include utilities that can override normal controls (such as all those listed above). The Information Asset Owner (eg system owner or individual with equivalent responsibilities) should ensure that all system utilities are identified, disabled where not necessary, and access to and use of any functional system utilities strictly controlled.

Session Time Out

13. Some systems incorporate time-outs that clear a session screen if activity has not taken place for a pre-determined time. On some sensitive systems the connection with the application/network is also terminated. The Information Asset Owner (eg system owner or individual with equivalent responsibilities) should ensure that a time-out assessment has taken place and suitable rules put in place.

Limitation of Connection Time

14. Some systems restrict user sessions to time slots eg the system can only be used between 0900hrs and 1300hrs. Others utilise maximum session periods eg remote access sessions last for four hours and are then terminated. The former control is rarely used in NHS systems. However, the latter is used quite commonly.

Information Access Restrictions

15. The integrity and availability of information is obviously important and should be considered by the Information Asset Owner (eg system owner or individual with equivalent responsibilities). The ‘need to know’ principle of access should be supplemented with additional controls for altering or deleting information. File storage systems should be constructed with these criteria in mind as, in many cases, access to a folder allows the user to view, alter, copy or delete files in the folder (and sub-folders) unless they are protected.

Sensitive System Isolation

16. Systems holding data that is considered sensitive should be physically and logically protected from unauthorised access. When looking at computer systems in NHS organisations it is difficult to define which systems should not be considered sensitive. The nature of the data, the relationship of the system to other systems and the network, and the location of the system all contribute to a variety of risks and threats that can have an impact on more than a single system or its data.

17. Patient/service user, personnel and financial data are all considered sensitive due to legislation, eg the Data Protection Act 1998 or commercial considerations. Systemic weaknesses in a system that does not contain sensitive data can lead to malicious code being transmitted to systems that do include sensitive data. Therefore, these criteria should be considered during the risk assessment for the system.

Legitimate Relationships

18. Legitimate relationships are a relatively new concept implemented in the NHS, arising from the development of the NHS Care Records System. Quite simply, legitimate relationships control who has authorised access to a patient's electronic care record.

19. The establishment of “Legitimate Relationships” will be required for NHS Trusts that are preparing to link to the national spine within the NHS CRS, as once the system is fully operational NHS CRS users will be unable to access a clinical record where there is no “legitimate relationship”.

20. Legitimate relationships are created between a patient and one or more ‘workgroups’ or teams of staff that are involved in providing them with care. They will generally be created behind the scenes eg as a consequence of an electronic referral or a registration process.

21. In some settings, eg general practice, it is relatively straightforward to determine the membership of a workgroup – in effect it will be all staff working for or with the practice, GPs, practice and community nurses, practice administrators and managers etc.

22. In larger, more complex Trust settings the assignment of staff to workgroups is a more complicated undertaking and will require robust planning. It is essential that the balance between safeguarding patient confidentiality and ensuring patient safety is maintained.

User Access Management

23. Organisations use a wide range of locally based information systems, from office electronic file storage to specialist departmental databases. Some systems may allow all members of staff access whilst others can restrict access to particular personnel. In all cases, it is essential that effective access management systems are in place, in order to prevent unauthorised access, loss or corruption of data, the introduction of malicious or unauthorised codes, the abuse of access rights, etc. This requirement applies equally to locally managed systems which process personal data and to those which do not.

24. In some organisations staff members are allowed to access the internet for limited private purposes, eg email or web browsing. Where this is allowed locally, the

conditions for personal use of such facilities should be defined within appropriate policy documents. The use of web email and the browsing of 'untrusted' web sites may potentially introduce risks, for example, the download of *malicious code* (spyware, viruses, worms, etc) or the viewing/sharing of inappropriate or illegal material. Therefore, it is essential that formal policies exist which detail staff obligations and undertakings for acceptable use.

25. Most information systems are now electronic and computer-based, however, paper-based, audio and video tape systems continue to be used, especially at departmental level. Regardless of media type, it is best practice that only authorised users should have access to these systems. Procedures for the following areas should be put in place.

User Registration

26. A system owner (for NHS Trusts this will be the Information Asset Owner (IAO)) should be identified in the system level security policy. The policy should also identify the need for and existence of a formal registration / deregistration procedure, with restricted authorisation for registering / deregistering users.

27. The registration process should ensure that the system can reliably identify the user. User authentication can vary in complexity depending on the sensitivity of the data to which the user may have access or depending upon the criticality of the system to the business of the organisation.

28. It is best practice that computerised system users should have a unique logon identity (ID), with a system and/or application log that shows logon/off times and activity. Some systems may by exception allow group IDs to be used locally. In such cases, it is impossible to attribute actions to an individual, so group IDs should be used only when absolutely necessary and where personal accountability is not an overriding issue.

29. User access rights should reflect the business needs of the user. For example, some users may only need to view data, but not change or add to it. Some systems are also granular, in that they only allow users to access data on a 'need to know' basis. For example, a receptionist who books appointments for a patient / service user only needs to confirm the person's identity and not see other data in the system relating to the individual's condition. Therefore, the local system administrator should establish user profiles and manage user rights based on the 'need to know' criteria.

30. Users should acknowledge (digitally, or in writing) 'acceptable terms of use' documentation or similar as part of the registration process. This should explain user rights in unambiguous terms and users should sign to acknowledge they have read, understood and agree to these terms.

31. User training documentation, guidance and the provision of user training sessions should also be an integral part of the user registration process.

32. The local system owner (for NHS Trusts this will be the IAO) should ensure that effective procedures are in place for deregistering users who no longer need access to the system eg they no longer work for the organisation or have changed jobs. For deregistration to work effectively, the system owner, supported by the system administrator (for NHS Trusts this will be the Information Asset Administrator (IAA)) should establish a formal agreement with the Human Resources department, to

ensure the latter provides timely details of leavers and movers to the former. This is especially important in the case of systems that include users from a range of departments, or in large departments, where the system's administrator is not routinely aware of user changes.

33. A procedure should be available for temporarily suspending user accounts. This procedure may apply to those who have lost their log-on credentials, are suspected of misusing the system or are on long-term sick or leave.

Privilege Management

34. System and database administrators/managers will typically have special system access rights that allow them to view and correct system data as part of a system's maintenance or potentially to amend data that other users have entered in error. This constitutes the basis of privilege management (also known as privileged users or superusers). Local system owners (or equivalently responsible individuals) should ensure that such high-privilege user accounts are kept to a minimum and that the actions of those using such accounts can be fully identified, and be auditable and actions accountable. For example, a group logon as 'administrator' and a common password should be avoided, since it is impossible to reliably audit activity.

User Password Management

35. Passwords are a common means by which a user is identified to the system and therefore password creation, distribution and use should be strictly controlled. If a password is being distributed electronically then it may be encrypted (this requires either an existing secure interface or an additional exchange process to allow the password to be decrypted by the intended user). Another option may be to deploy an ID token that can generate a random one-time password or unique number that is synchronised with the system to be accessed.

36. It is well documented and acknowledged that the proliferation of system passwords leads to control weakness by their owners, eg password sharing or loan, writing down passwords, changing all passwords to the same common value. The fewer passwords assigned to each user the better and indeed some organisations have implemented a single sign-on approach whereby a user need only control a single set of credentials. User access rights should be reviewed at regular intervals and the process detailed within organisational access control procedures. This ensures that the access rights applicable to an individual are still appropriate to their organisational role.

37. Systems are best configured to ensure that initial passwords issued to their users have to be changed during the system's first access and regularly thereafter.

38. User passwords should be robust. As a minimum, passwords should be no fewer than 6 characters, alphanumeric (mixture of letters, numbers and special characters e.g. 5a!!AcY), non-consecutive, (eg Pa55w0rD1 followed by Pa55w0rD2 would not be allowed) and minimum enforced change periods established. A recommended solution would be to use memory tricks to help create memorable, but hard to guess passwords. For example, make a password out of the first letters of each word in a memorable phrase. "Somewhere over the rainbow way up high" (sotrwuh). Then by adding a mixture of upper and lower case with numbers and special characters included to produce; S0trw^h1gh

39. Some systems may employ configurable password construction and management standards that exceed this basic level. Users should also be provided with the opportunity to change their passwords more frequently, if they wish.

40. System users should be issued with written guidance on password confidentiality, construction, changing, storage and what to do when they forget a password. The guidance should also include instructions for reporting suspected password / identity misuse or theft or the loss of log-on devices.

Review of User Access Rights

41. The local Information Asset Owner (eg system owner or equivalently responsible individual) should ensure a written procedure is developed to regularly review all system user access rights. The review should be used to ensure users remain active and their access rights are allocated correctly. Six months is the recommended maximum period between such reviews although access reviews are best undertaken on a frequent basis and may be aligned with staff recruitment or movement cycles.

42. Privilege rights should also be reviewed frequently. Three months is the recommended maximum period between reviews.

Social Networking and Blogging

43. In some organisations there have been considerations for the potential applications of social networking type services that may be accessed and used by service users and staff. Where such services are locally required and approved, care must be taken to ensure the information risks and management implications are appropriately considered. Specific NHS IG guidance is available on this topic and will assist NHS organisations to develop and implement an effective management approach that supports their business needs. See the **Knowledge Base Resources**.

Unattended User Equipment and Data

44. A ‘clear desk and screen’ policy should be adopted for the system to ensure data is protected from unauthorised access. The organisation’s Information Security and / or Information Governance policy should include a clear desk and screen clause for all systems and data. If this is not the case, the system owner should ensure such a clause is included in the system’s policy document. System training modules and written procedures should include guidance to ensure the policy is implemented effectively.

45. Users should lock access to their workstations when they are not using them at periods during the day, through the use of a password screensaver and / or by removing any provided access management device such as a Smartcard. Local guidance on the mechanisms to be used should be provided.

46. Paper and other media should also be locked away when not in use. This is especially important for media that contain personal details or other sensitive information.

47. Fax machines should be located so that unauthorised users cannot see any data sent to the machine. In the case of fax machines that receive / send personal data

the principles of a safe haven (see **requirement 308**) should be put in place. For more information refer to Fax, Printer Ribbons and Cartridges Guidance

48. Photocopiers and other multi-function office systems should be secured so that only authorised personnel may use them, eg password access systems. Digital copiers containing hard-drives should be controlled in the same manner as required for other digital media, eg secure disposal.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013
DH: NHS IG - Information Risk Management - Good Practice Guide 2009	This guidance is aimed at those responsible for managing information risk within NHS organisations. It reflects government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures in Government'. This GPG also includes guidance on the need for Forensic Readiness Policy and local implementation.	24/01/2013
DH: NHS IG - Blogging and Social Networking 2009 (PDF, 53 KB)	IG Policy team guidance that provides NHS organisations with a general awareness of the associated risks of blogging and social networking that may potentially affect the effectiveness of local services.	24/01/2013
HSCIC: Good Practice Guidelines - Application Security	This guide covers various general user applications and their security.	24/01/2013
HSCIC: Good Practice Guidelines in Information Governance - Information Security	The Good Practice Guidelines (GPG) are a series of informational documents which provide best practice advice in technology specific areas of Information Security.	24/01/2013

Electronic Social Care Record (ESCR)	This briefing defines the content of the Electronic Social Care Record (ESCR) and outlines the background and current developments in implementation.	24/01/2013
DH: Defining the Electronic Social Care Record (PDF, 2883 KB)	The document provides a non-technical introduction to the concept of the electronic social care record.	24/01/2013
BS ISO/IEC 27000 Series of Information Security Standards	Note that only NHS Information Governance Toolkit (IGT) administrators may download a copy of the standards for use by their organisation. The administrator must be logged on to download these standards.	24/01/2013
DH_NHS IG - Fax Printer Ribbons and Cartridges Guidance (PDF, 49 KB)	This Information Governance (IG) guidance provides NHS organisations with a general awareness of the associated risks for maintenance and disposal of fax printers and other devices that use consumable ribbon or film. It should be read in conjunction with the NHS IG Risk Management Guidance for Maintenance and Secure Disposal of Digital Printers, Copiers and Multi Function Devices.	24/01/2013
DHID: AQP (Clinical) Template - Compliance Monitoring Form (DOC, 50 KB)	A form to assist organisations to check whether their staff are complying with procedures.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
DH: NHS IG - IG Checklist for Staff Movers and Leavers 2008 (DOC, 44 KB)	This NHS IG leavers checklist should be considered for staff who are leaving their NHS employment or who may be moving to another position within the organisation.	24/01/2013
DH: NHS IG - Email Policy (DOC, 111 KB)	This document sets out an organisation's policy for the protection of the confidentiality, integrity and availability of the email system; establishes organisation and user responsibilities for the email system and provides reference to documentation relevant to this policy.	24/01/2013

DH: NHS IG - User Guide to Passwords (DOC, 36 KB)	Detailed guidance for users on creating and protecting their passwords.	24/01/2013
DH: NHS IG - Internet Use Policy (DOC, 82 KB)	A template that sets out an organisation's policy for the protection of the confidentiality, integrity and availability of the Internet system and establishes organisation and user responsibilities for the Internet system.	24/01/2013
Bite-sized Good Practice Guide: Safe Computing (DOC, 347 KB)	IG Policy team leaflet on good practice in safe computing.	24/01/2013
Bite-sized Good Practice Guide: Internet and Email (DOC, 393 KB)	IG Policy team leaflet on good practice in using the internet and email.	24/01/2013
Walton Centre: Access and Authentication Standard (Network) (PDF, 140 KB)	Standards and procedures outlining the way in which an organisation is able to prevent unauthorised access to network assets.	24/01/2013
Walton Centre: Monitoring & Audit Standard (PDF, 239 KB)	A procedure to enable the monitoring of information flows within as well as into and out of the organisation.	24/01/2013
Walton Centre: Full Information Security Management System (DOC, 35 KB)	Walton Centre For Neurology & Neurosurgery NHS Trust - Full Information Security Management System.	24/01/2013
Corporate Information Security Policy Template (DOC, 98 KB)	A template providing organisations with an illustrative template Corporate Information Security Policy as a model for constructing their own policies.	24/01/2013
System Level Security Policy (SLSP) (DOC, 47 KB)	A template for defining system level security arrangements. This template is relevant to the NHS Information Risk Management Good Practice Guide. It should be read in conjunction with the section specifically addressing security policy.	24/01/2013
IT Operations: Monitoring Systems Access & Use (PDF, 261 KB)	Processes for monitoring access to and use of systems including event logging and analysis.	24/01/2013
IT Operations: Enforced Path Policy (PDF, 34 KB)	A policy setting out a mechanism to ensure that end-users only have access to those application and data areas for which they are authorised	24/01/2013

IT Operations: Review of User Privileges (RTF, 328 KB)	A template for performing reviews of access to systems and checking that all users listed for those systems still require their current access level.	24/01/2013
IT Operations: User Access Management Policies (PDF, 33 KB)	The policy describes the registration and de-registration process for information systems and services.	24/01/2013
Nottingham: Information Security - Hardware & Software Guidelines (PDF, 196 KB)	Leaflet on Information Security Hardware and Software usage for users.	24/01/2013
Nottingham: Information Security and Password Guidelines (PDF, 167 KB)	Leaflet for system users that defines Information Security and gives advice on creating secure passwords.	24/01/2013
Information Security Forum: Security Staff Remote Access - Implementation Guide (PDF, 4424 KB)	(NHS Network users only): 154 page document setting out practical guidance on securing remote access for staff, it contains 10 implementation steps, each providing useful background information and supporting material (for example, a checklist, a sample policy or a summary of controls)	24/01/2013
Information Security Forum: Security Staff Remote Access - Risks and Controls (PDF, 3072 KB)	(NHS Network users only): 79 page document setting out the risks in providing remote access to staff and guidance on common controls to minimise the risks	24/01/2013
DHID: AQP Template - Compliance Monitoring Form (DOC, 50 KB)	A form to assist organisations to check whether their staff are complying with procedures.	24/01/2013
DHID: AQP Template - Access Control Procedures (DOC, 66 KB)	A template on managing access to computer systems.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **Password Management** - an introductory module on protecting sensitive data by choosing a good password.
- **Information Security Guidelines** - an introductory module on keeping information secure in and out of the workplace.

- **Secure Transfers of Personal Data** - a foundation level module that informs learners how to protect sensitive data from unauthorised access and accidental loss, damage or destruction during transfer and how to dispose of sensitive data when it is no longer needed.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- ISO/IEC27002: 2005 controls ref 11.1, 11.2, 11.3, 11.5, 11.6
- Protecting and Using Patient Information, Caldicott Management Audit point 17 - User responsibilities and 18 Access controls
- The Caldicott Report - Principle 4: Access to patient-identifiable information should be on a strict need-to-know basis
- Principle 7 of the Data Protection Act 1998
- The NHS Care Record Guarantee, Commitments 10 and 11

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**There are documented requirements for access controls for all key information assets. Access rights for specific individuals/groups have been agreed and documented in relation to these information assets.**		
	a	Responsibility for defining and documenting requirements for both system and user access controls have been assigned to appropriate staff/senior management. **Evidence Required:** • Named individuals' job description(s), or notes or e-mails assigning responsibility or the terms of reference for groups who approve access (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	b	Operational, managerial and technical security access controls have been defined, documented and approved for each key information asset. Access rights for groups of staff and individual current users of information assets have been defined, documented and approved. **Evidence Required:** • System Level Security Policies, access control requirement specifications or system design documents (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
2	**There are appropriate user access management procedures (including user registration, update and deregistration processes), technical functionality and management controls for all key information assets.**		
	a	IAOs or equivalent have ensured that there are approved access controls in place for each key information asset under their control. **Evidence Required:** • Reports generated by system utilities, procedures, system documentation or system configuration details (eg password strength settings, threshold for number of failed login attempts etc) (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	

	b	Access to information assets is only possible for individuals who have been duly authorised. **Evidence Required:** • Security reports, access log files generated by the system, the Information Asset's System Level Security Policy and associated access management procedures such as user registration and deregistration including temporary access (eg contractors/visitors; signatures/electronic evidence of authorisations; the disabling and erasure of unused accounts; disabling of access to files that are no longer required for current staff positions) (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate). **Notes/other evidence:**	❑
3	**Regular reviews are carried out to audit and assure the access control and management processes. Prompt action is taken to update, replace, disable or remove profiles and individual accounts. Regular assurance reports are provided to the SIRO (or individual with equivalent responsibilities).**		
	a	Documented reviews and audits are carried out to assure the effectiveness of security access control and management processes. **Evidence Required:** • Minutes/meeting notes where the security access control and management processes have been reviewed including the decisions made and any updates. **Notes/other evidence:**	❑
	b	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. **Evidence Required:** • Reports from monitoring software, audit reports (for example checking what access people have, and compliance), reports to a SIRO or equivalent, notes or minutes from review meetings, evidence of disabling and erasure of accounts may be found within automated system records, auditable log files, comparison of deregistration against HR leavers' records or within records kept as part of an Information Asset document. **Notes/other evidence:**	❑
	c	[Level 3 Maintenance - only required if Level 3 achieved in previous year] The robustness of security and access controls may change over time. It is therefore important that the appropriateness of the access control functionality of information assets is regularly reviewed and maintained. **Evidence Required:** • Periodic reports (eg by the IAO or equivalent), follow up actions resulting from audit findings and updates to any relevant policy or procedure. **Notes/other evidence:**	❑

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Requirement No:	11-313
	Initiative:	Information Security Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

The objective of this requirement is to ensure there is appropriate protection for information communicated over local networks and for the protection of the supporting infrastructure (including wireless networks).

Security of Communication Networks

Introduction

1. The secure operation of networks, which may span organisational boundaries and beyond, requires that careful consideration be given to management, dataflows, legal implications, monitoring, and protection. Additional controls may also be required to protect sensitive information passing over public networks.

Information Assets: Network Controls

2. Network controls should exist to protect the local network from threats to its components. This includes the systems and applications using the network, as well as the information passing through it, and the level of access permitted. To ensure good network security the following should be considered:
    a. the assigned individual responsible for the asset (in NHS Trusts this will be the nominated *Information Asset Owner* (IAO)) should ensure there is a Network Security policy;
    b. network operational management responsibility should be separated from desktop computer operations. This helps protect against possible conflict of interest and may help with problem management;
    c. procedures should be established for the management of remote equipment owned by the organisation. This includes portable and fixed remote equipment (see **requirement 314**);
    d. establish controls to protect the confidentiality and integrity of data passing over public (eg World Wide Web) or wireless networks;
    e. logging and monitoring of all network activity.

Security of Network Services

3. Network services (in-house or provided externally) should normally be subject to service level agreements or contracts, and the security features for the service

identified, defined, with the responsibility for maintenance, monitoring and reviewing of security features agreed by the nominated IAO (or individual with equivalent responsibilities). The organisation should ensure it includes the right to audit the services provided as part of the agreement.

4. Security features should be identified through risk assessment processes and subject to regular review and where necessary, refinement. Typical security features to be considered include:

   a. authentication, encryption and network connection controls;

   b. technical parameters required for secure network connections;

   c. access approval, restriction and revocation procedures;

   d. anti-virus / malicious code detection, removal and prevention procedures;

   e. environmental controls to protect network equipment, ie from fire, flood etc.

5. Where a network connects to the NHS national network (*N3*), it is essential that the information security management standards applied to the local network are sufficient to prevent onward threats arising to the N3 or the information assets of its other connected organisations. This includes the implementation and management of effective anti-virus measures and, where necessary, firewalls. Comprehensive network security requirements are provided and assured by NHS Connecting for Health, through its *Information Governance Statement of Compliance* (IGSoC) processes and related Information Governance security guidance, for the benefit of all organisations that use the N3. Failure to observe these N3 information security standards may potentially prevent the local network being allowed to access other important NHS information assets.

   Please note - it is best practice to ensure that any suppliers to the organisation also adhere to this requirement.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013

DH: NHS IG - Information Risk Management - Good Practice Guide 2009	This guidance is aimed at those responsible for managing information risk within NHS organisations. It reflects government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures in Government'. This GPG also includes guidance on the need for Forensic Readiness Policy and local implementation.	24/01/2013
HSCIC: Good Practice Guidelines in Information Governance - Information Security	The Good Practice Guidelines (GPG) are a series of informational documents which provide best practice advice in technology specific areas of Information Security.	24/01/2013
BS ISO/IEC 27000 Series of Information Security Standards	Note that only NHS Information Governance Toolkit (IGT) administrators may download a copy of the standards for use by their organisation. The administrator must be logged on to download these standards.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Walton Centre: Communications Standard (PDF, 120 KB)	The document includes requirements for network protection, cabling, wireless connection, remote communications and compliance.	24/01/2013
Walton Centre: Full Information Security Management System (DOC, 35 KB)	Walton Centre For Neurology & Neurosurgery NHS Trust - Full Information Security Management System.	24/01/2013
DH: NHS IG - Network Security Policy 2003 (DOC, 90 KB)	A template to assist organisations to define a Network Security Policy.	24/01/2013
DH: NHS IG - Internet Use Policy (DOC, 82 KB)	A template that sets out an organisation's policy for the protection of the confidentiality, integrity and availability of the Internet system and establishes organisation and user responsibilities for the Internet system.	24/01/2013

System Level Security Policy (SLSP) (DOC, 47 KB)	A template for defining system level security arrangements. This template is relevant to the NHS Information Risk Management Good Practice Guide. It should be read in conjunction with the section specifically addressing security policy.	24/01/2013
IT Operations: User Access Management Policies (PDF, 33 KB)	The policy describes the registration and de-registration process for information systems and services.	24/01/2013
IT Operations: Document Operating Procedures (RTF, 223 KB)	The purpose of this document is to give a broad outline of the various aspects of Information Security Procedures, guiding the users to more specific processes applicable to the systems used in the NHS Purchasing and Supply Trust.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of information risk management. Staff whose roles involve the handling of personal data will benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.
- **NHS Information Risk Management** - a foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- Principle 7 of the Data Protection Act 1998

- BS ISO/IEC 27002:2005, controls 10.1.1 - 4, 10.3, 12.1 Communication and Operation Management (Procedures)
- BS ISO/IEC 27002:2005, controls 10.6 - Network Security Management

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**IAO's or equivalent responsible for ICT networks have reviewed Information Security risks. Responsibility for network security has been assigned to an IAO (or equivalent) who undertakes reviews of information security risks. Mitigating procedures, controls and responsibilities are identified and documented.**		
	a	A network security policy has been produced for each ICT network and approved by the SIRO or equivalent. **Evidence Required:** • Documented network security policy /policies (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate). • Approval may be in minutes of meetings, in a document or email or a personal endorsement in writing from the SIRO or equivalent (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	b	Information Asset Owners (or equivalent) responsible for information communication technology (ICT) networks, undertake reviews of information security risk in relation to those networks, and the controls and procedures required to mitigate these risks in accordance with the Network Security Policy. **Evidence Required:** • Risk review documentation, security policies, documented procedures and/or risk management plan (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	c	Network security controls and procedures that mitigate against risks are approved by the Senior Information Risk Owner (SIRO) or equivalent senior manager or committee. **Evidence Required:** • Minutes/meeting notes or a note of endorsement from the SIRO or equivalent (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	

2	**The approved procedures and controls for network security in respect of all information networks controlled by the organisation have been implemented.**		
	a	The identified controls and procedures have been implemented in respect of all ICT networks in accordance with policy. **Evidence Required:** • A single document which identifies the controls applied, such as network capacity planning, network security, reliable firewalls, gateways and domains and file storage facilities supporting individual and group access (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	b	The documented and approved procedures and controls have been made available at appropriate points in the organisation and all relevant staff have been informed of their responsibilities to maintain network security by complying with them. Informing staff might be done through team meetings, staff briefings, awareness sessions and by IT user induction training. **Evidence Required:** • Publication of procedures on the intranet, or hard copy procedures available in departmental procedures folders, or inclusion in staff handbook (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate). • Notes/minutes of team meetings/awareness sessions or staff briefing/training materials (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
3	**Compliance with the implemented network security controls and procedures is monitored, and remedial or improvement action is promptly taken. Regular security risk reviews and assurance reports are provided to the SIRO (or equivalent).**		
	a	Compliance with the network security policy is monitored and where necessary, prompt remedial or improvement is action taken. **Evidence Required:** • Reports of the outcome of staff spot checks, monitoring software, results from audits (including technical) and penetration testing, and checks of system documentation and functionality. • Implementation of new controls, reconfigured controls, or new guidance for staff.	❑
		Notes/other evidence:	
	b	Regular security risk reviews and assurance reports are provided to the SIRO (or equivalent). **Evidence Required:** • Formal reports, briefing notes, or minutes of meetings where network security was discussed.	❑
		Notes/other evidence:	

	c	[Level 3 Maintenance - only required if Level 3 achieved in previous year] Existing policy and associated procedures and controls must be regularly reviewed to ensure that ICT networks continue to operate securely. **Evidence Required:** • Minutes/meeting notes where the procedures or controls have been reviewed including the decisions made and any updates to the documentation or controls.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

Policy and procedures ensure that mobile computing and teleworking are secure	Requirement No:	11-314
	Initiative:	Information Security Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

Mobile computing and *teleworking* pose a substantial risk. For example, devices may be lost, damaged, or stolen, potentially resulting in the loss or inappropriate disclosure of data. The information security protection measures required should be commensurate with the risks presented by these working arrangements.

Security of Remote Working and Mobile Computing

Introduction

1. When using mobile computing, the risks of working in an unprotected environment must be considered and mitigated where possible by the use of appropriate security procedures or facilities. In the case of teleworking, the organisation should assess the risks involved and apply proportionate security controls to mitigate these risks. Documented and agreed working procedures, describing best practice, should be in place to ensure staff working remotely, do so safely and securely. It is essential that the individual assigned responsibility for the asset (in NHS Trusts this will be the responsible *Information Asset Owner* (IAO)) is aware of, and has approved in advance, the use of mobile working for the information assets they are responsible for - (see **requirement 307 or 316** dependent on organisation-type).

Mobile Computing and Remote Communications

2. The use of portable devices and mobile computing equipment is now commonplace in many organisations, with users connecting remotely to required information services through laptops, mobile phones, palmtops, smartphones, Blackberry's etc. Users are also connecting from a variety of locations – home, hotels, NHS and council premises, and through internet, wireless and dial-in technologies. Therefore, it is essential that the following are considered within a risk assessment:

    a. **Theft, Loss or Damage of Equipment.** Equipment in transit is at particular risk of being damaged, lost or stolen. This is especially the case for equipment used by authorised mobile workers who are likely to connect to information systems from a number and variety of locations. Training, procedures and written guidance must be put in place for users, to cover these threats.

    b. **Unauthorised Access to Data.** Unauthorised access is possible in a number of ways. Users may leave portable devices, computer equipment or media

containing data unattended in a place where it may be seen or used by unauthorised individuals.

c. ***Encryption*.** As a consequence of the November 2008 Cabinet Office Data Handling Review report (see NHS Chief Executive David Nicholson letters available from the **Knowledge Base Resources**), all public sector organisations are now mandated to ensure any digital information that is either person identifiable or otherwise sensitive, is encrypted to appropriate NHS standards. This mandate applies to both the storage of, and transfer of any such digitally held information.

d. **Technical Hacking/Cracking.** The implementation of appropriate policy statements and supporting procedures (see **requirement 305** dependent on organisation-type), together with user training, can help mitigate this risk. Unauthorised use can be gained through technical means, eg through 'network sniffing' or through guessed passwords on unattended or unprotected laptops. Encrypted data on media, encrypted transfer, strong access controls, user identification and authentication and secured wireless networks should all be considered to counter opportunist technical hacking / cracking. It is recommended that 'two factor' authentication is used and token-based, biometric, smartcard, etc controls are implemented as in nationally provided NHS applications through the use of Smartcards.

e. **Malicious and Unauthorised Mobile Code.** (see also **requirement 311** dependent on organisation-type). Care must be taken to ensure that all mobile devices and removable media have their *anti-virus* / anti-spyware components regularly updated to protect against these types of attacks. "On access" file scanning should also be enabled within anti-virus products, to help detect email messages containing *malicious code*, or infected files transferred from other storage media.

f. **Data Backups.** Data stored on local drives (eg laptop hard disk) may be vulnerable to loss or corruption. If data is merely saved to a local drive and the device is lost, then so is the data. The minimum amount of data required must be carried on mobile devices to reduce the potential impacts of an unforeseen event. Master copies of documents should never be stored on local disk drives; only copies of information should be taken 'off-site'.

g. **Mobile Working Policy.** The organisation should have a documented policy (and supporting procedures) that covers all aspects of mobile working. If teleworking or homeworking is allowed by the organisation then the security, management arrangements and user requirements for this must also be covered in the organisation's policy.

Seeking an exemption from the requirement

3. To obtain an exemption from the requirement, an email should be sent to the Exeter Service Desk (exeter.helpdesk@hscic.gov.uk) with the following statement confirmation, and include your name and organisation details: **Organisation name (organisation code) has made an assessment of mobile computing use and personal information is NOT recorded, viewed, transferred and stored on tapes (including back-up tapes), PDAs, laptops, mobile phones, memory sticks or equivalent mobile computing equipment**.

4. **Note:**If an assessment has been made and no mobile computing systems including back-up tapes, PDAs, laptops, mobile phones, memory sticks or equivalent mobile computing equipment are used to access or view patient/service user information, this should be recorded for audit purposes.

Teleworking and Homeworking

5. Teleworking / homeworking is distinct from mobile working in that the location is normally fixed (eg the staff member's home). The criteria listed above apply to teleworking and the following should also be considered within a risk assessment:

    a. **The Physical Security of the Location.** The risks of home burglary must be considered and organisations may choose to implement a separate teleworking / homeworking policy. However, the information security issues may potentially be addressed through a unified mobile working policy. Therefore, the use of additional physical security devices (eg Kensington locks, anchorpad encasements) must be considered.

    b. **The Environmental Conditions.** (for certain organisation types see also **requirement 10-310**). Employers have health and safety obligations to teleworkers that include assessing the environment to ensure teleworking equipment does not pose a threat to the teleworker's property, the teleworker's person, or to third persons. Equally, the environment should be assessed to ensure it does not pose a threat to the organisation's equipment or business functions, for example, poor ventilation resulting in overheating and loss of access or service capability. The organisation's Health & Safety manager (or equivalent) should ensure an environmental assessment procedure and checklist is developed and completed before teleworking commences.

    c. **Equipment Ownership.** The organisation should ensure that it provides necessary workstations and associated equipment for business use. The use of employee-owned equipment should be avoided as other family members may access it for private purposes thus increasing risks of unauthorised access to data. The policy should include a provision that specifies official equipment is not to be used by unauthorised users or for unauthorised purposes, and guidance issued.

    d. **Employer Insurance.** The organisation will have to ensure that adequate insurance cover is available for teleworkers and that covers any equipment on a teleworker's premises. Cover is normally available within the homeworker's normal home contents insurance.

    Please note - it is best practice to ensure that any suppliers to the organisation also adhere to this requirement.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013
David Nicholson Communications	Letters from the NHS Chief Executive to all local NHS Trust Chief Executive Officers, regarding the impact of the Cabinet Office Data Handling Review upon the NHS.	24/01/2013
DH: NHS IG - Good Practice Guide for the Transfer of Batched Person Identifiable Data	Good Practice Guidelines for the transfer of batched person identifiable data by means of portable electronic media. These equally apply to back ups and data destruction.	24/01/2013
HSCIC: NHS Encryption Tool	Information about how to request the NHS encryption tool, arrange training and gain access to support and updates.	24/01/2013
Guidance on the Implementation of Encryption within NHS Organisations	(NHS Network users only): The guidance is provided to assist NHS IM&T managers and business owners in the selection and implementation of encryption solutions within their organisation.	24/01/2013
BS ISO/IEC 27000 Series of Information Security Standards	Note that only NHS Information Governance Toolkit (IGT) administrators may download a copy of the standards for use by their organisation. The administrator must be logged on to download these standards.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
DH: NHS IG - Remote Access Policy 2003 (DOC, 74 KB)	A template to assist organisations to define a Remote Access Policy.	24/01/2013
DH: NHS IG - Laptop Security Policy 2008 (DOC, 66 KB)	IG Policy team document which is recommended for adoption by NHS organisations of all types where laptop computers are used. The policy is equally applicable to NHS contractors, services providers and other organisations or agencies that use laptop computers to process NHS information in the performance of their duties.	24/01/2013
DH: NHS IG - Home Working Policy and Procedural Template 2008 (DOC, 44 KB)	IG Policy team document and template to manage and prevent unacceptable risks arising to the organisation and other NHS information assets through the use of unapproved or unsafe home working facilities.	24/01/2013
Walton Centre: Remote Working Standard (PDF, 121 KB)	The document outlines the control procedures in place for remote working, including approval, connection method, access control and authentication.	24/01/2013
Walton Centre: Communications Standard (PDF, 120 KB)	The document includes requirements for network protection, cabling, wireless connection, remote communications and compliance.	24/01/2013
Walton Centre: Full Information Security Management System (DOC, 35 KB)	Walton Centre For Neurology & Neurosurgery NHS Trust - Full Information Security Management System.	24/01/2013
Bite-sized Good Practice Guide: Mobile Computing (DOC, 337 KB)	IG Policy team leaflet on good practice in mobile computing.	24/01/2013
Audit Programme - Mobile and Remote Working (DOC, 67 KB)	A checklist to assist organisations to monitor compliance with mobile and remote working procedures.	24/01/2013
IT Operations: User Access Management Policies (PDF, 33 KB)	The policy describes the registration and de-registration process for information systems and services.	24/01/2013

IT Operations: Review of User Privileges (RTF, 328 KB)	A template for performing reviews of access to systems and checking that all users listed for those systems still require their current access level.	24/01/2013
DHID: AQP Template - Assignment of Mobile Computing Equipment Form (DOC, 37 KB)	A template to ensure that only authorised staff members have access to computing equipment and to ensure they sign to say they are aware of the risks of mobile computing and will comply with confidentiality and security measures.	24/01/2013
DHID: AQP Template - Mobile Computing Equipment Asset Log (DOC, 44 KB)	A template to record the allocation of mobile computing equipment.	24/01/2013
DHID: AQP Template - Staff Guidelines on Using Mobile Computing Equipment (DOC, 46 KB)	Guidelines for staff on the safe use of mobile computing devices.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Business Link: Employees working from home	Guidance setting out the key issues and considerations when introducing and managing home-working.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of information risk management. Staff whose roles involve the handling of personal data will benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.
- **NHS Information Risk Management** - a foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.
- **NHS Information Risk Management for SIROs and IAOs** - an introductory module that describes key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties. SIROs should also review the IRM Foundation module.

- **Password Management** - an introductory module on protecting sensitive data by choosing a good password.
- **Information Security Guidelines** - an introductory module on keeping information secure in and out of the workplace.
- **Secure Transfers of Personal Data** - a foundation level module that informs learners how to protect sensitive data from unauthorised access and accidental loss, damage or destruction during transfer and how to dispose of sensitive data when it is no longer needed.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- ISO/IEC 27002 (revised 2005) controls ref 11.7
- Principle 7 of the Data Protection Act 1998

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**The IAO (or equivalent) ensures there is a documented policy for approvals and authorisation for mobile working and teleworking arrangements. The procedure is supported by documented guidelines for staff on expected NHS IG information security and confidentiality practice.**		
	a	There are documented procedures for mobile working or teleworking that provide guidelines for staff on expected behaviours. **Evidence Required:** • Documented mobile or teleworking procedures (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	b	There is a documented policy for approvals and authorisation for mobile working and teleworking arrangements. **Evidence Required:** • Documented policy for approvals and authorisation for mobile and teleworking (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	c	The documented approvals policy and procedures have been agreed by an appropriate senior manager or group. **Evidence Required:** • Minutes of meetings, in a document or email or a personal endorsement in writing of the approvals policy and procedures from an appropriately senior manager or group (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
2	**All mobile or teleworkers are appropriately approved, authorised and made aware of procedures/guidelines. Robust remote access solutions and adequate information security functionality for mobile devices and removable media has been provided.**		
	a	All mobile or teleworkers are appropriately approved and authorised, and records are maintained of all authorisations (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate). **Evidence Required:** • Records of approval, signatures/electronic evidence of authorisations, the removal of authorisation for unused accounts.	❑
		Notes/other evidence:	

	b	Mobile or teleworkers are provided with procedures / guidelines. **Evidence Required:** • In staff handbook, publication of procedures on the intranet, hard copy procedures provided to relevant staff, briefing materials, or awareness session materials (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate).	❑
		Notes/other evidence:	
	c	Robust remote access solutions have been provided (**For Local Authorities Only: -** This could be a copy of the Current PSN CoCo certificate). **Evidence Required:** • Technical specification documentation relating to the solution itself. • System reports detailing number of users and the equipment allocated to them.	❑
		Notes/other evidence:	
3	**There are regular reviews to audit and monitor mobile and/or teleworking arrangements and the remote working procedures and controls. Where a need for improvement or non-compliance is identified this is documented and appropriate action taken.**		
	a	Providing staff with guidelines, procedures and briefings does not provide sufficient assurance that they have been understood and are being followed, therefore compliance spot checks and routine monitoring are conducted. **Evidence Required:** • Completed monitoring forms, or a report on the outcome of staff compliance checks.	❑
		Notes/other evidence:	
	b	Documented reviews are carried out to obtain assurance that the mobile and/or teleworking arrangements are only available to authorised users, all mobile devices and removable media are accounted for; secure remote access is in place and that sensitive or confidential information (including service user information) is encrypted, securely transported or stored in secure locations. **Evidence Required:** • Monitoring software, audit reports, reports to a SIRO or equivalent, and improvement plans.	❑
		Notes/other evidence:	
	c	[Level 3 Maintenance - only required if Level 3 achieved in previous year] The robustness of security and remote access controls may change over time. It is therefore important that the remote working procedures and guidelines are regularly reviewed to ensure they continue to be effective. **Evidence Required:** • Minutes/meeting notes where the procedures or controls have been reviewed including the decisions made and any updates to the procedures or controls.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

There is an information asset register that includes all key information, software, hardware and services	Requirement No:	11-316
	Initiative:	Information Security Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

The objective here is to account for *information assets* containing patient/service user information to ensure that in the event of damage, destruction or loss, there is awareness of what information is affected and, in the case of loss, whether the information held on the asset is protected from unauthorised access.

Information Asset Register

Introduction

1. Unless organisations know the type of information assets they possess it will be more difficult to ensure that each item is adequately protected through appropriate confidentiality and security measures.
2. Recording this information will also assist if an organisation needs to make a claim on their insurance for loss or damage to any of their assets.
3. The scope of the requirement is assets that hold or provide access to NHS patient information, or in the case of third/voluntary sector organisations - to service user information.

Categories of Information Assets

4. There are many types of information asset, but the initial focus should be on the four major categories below;
    a. **Information:** Patient databases, system documents and procedures, archived information etc.
    b. **Software:** Applications, system, development tools and utilities.
    c. **Physical:** Equipment such as PCs, laptops, PDAs, memory sticks, smartphones.
    d. **Services:** Computing and communications.
5. Assets should be written down and kept in the form of a simple register. There are no mandatory requirements for how the register should be structured, however it should be ensured that useful information is captured to enable compliance with the objective of this requirement.
6. For example the entry for a physical asset such as a computer will include:

a. its physical location, ie what part of the organisation it is in (with portable equipment the member of staff it has been assigned to - see also **requirement 318** or **requirement 314**, depending on organisation-type);

b. what software and information is included on it;

c. those responsible for the maintenance of the computer;

d. how to contact them if something goes wrong;

e. if it is linked to an Uninterrupted Power Supply (UPS) system; and

f. any Business Continuity Plans for recovery (depending on organisation-type see also **requirement 319**).

Information Asset Owners

7. An information asset owner is a senior member of staff that has overall responsibility for an information asset. The responsibility should ideally be linked to a post rather than to a person, as such responsibilities tend not to get passed on when an individual leaves the organisation or changes jobs within it.

8. The role of information asset owner is likely to be delegated to the IG lead or equivalent, (although ultimate responsibility will still rest with the owner, NHS contractor or Chief Executive). The asset owner should compile a list of information assets (ie what information is held, what is added and what is removed, how information is moved, and who has access and why) and identify any risks to the information. This will enable the risks to be addressed and ensure that use of information complies with legal and other obligations.

9. The information asset owner can assign day to day responsibility for a particular information asset to someone else (eg an employee who has sole use of a laptop). They should also be aware of any assets that are not the sole responsibility of the organisation, eg equipment that is leased or shared in use.

10. 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 a *commissioning organisation* during monitoring visits. Commissioning organisations will however want to have some evidence that the register exists and is up to date, for example details about the date the register was last updated and where it is stored. Please note that it is best practice to ensure that any suppliers to the organisation also adhere to this requirement.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013
DH: NHS IG - Information Risk Management - Good Practice Guide 2009	This guidance is aimed at those responsible for managing information risk within NHS organisations. It reflects government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures in Government'. This GPG also includes guidance on the need for Forensic Readiness Policy and local implementation.	24/01/2013
BS ISO/IEC 27000 Series of Information Security Standards	Note that only NHS Information Governance Toolkit (IGT) administrators may download a copy of the standards for use by their organisation. The administrator must be logged on to download these standards.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Dental practice template: Information Asset Register (DOC, 78 KB)	A template to enable the recording of information assets developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013

Pharmacy template: Information Asset Register (Word version) (DOC, 51 KB)	A template to enable the recording of information assets, developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, the Department of Health and IG leads in the NHS.	24/01/2013
Pharmacy template: Information Asset Register (Excel version) (XLS, 79 KB)	A template to enable the recording of information assets, developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, the Department of Health and IG leads in the NHS.	24/01/2013
Walton Centre: Asset Management Standard (PDF, 128 KB)	This document outlines the standards and procedures for the recording, control, auditing, and disposal of information assets. It also includes standards and procedures for change control and hardware updates.	24/01/2013
IG Resource Pack	These useful resources comprise staff awareness leaflets, exemplars, templates and model documents. Practices should scroll down the page for GP requirement specific resources.	24/01/2013
Bite-sized Good Practice Guide: Media Disposal (DOC, 313 KB)	IG Policy team leaflet on good practice on secure disposal of media on hard disk drives, CDs/DVDs, floppy disks and magnetic tapes, usb memory sticks and paper.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Pharmaceutical Services Negotiating Committee: IG Web Pages	Information for community pharmacy on NHS Information Governance - the IG training booklet can be downloaded from this site.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of information risk management. Staff whose roles involve the handling of personal data will benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.
- **NHS Information Risk Management** - a foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.
- **NHS Information Risk Management for SIROs and IAOs** - an introductory module that describes key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties. SIROs should also review the IRM Foundation module.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- ISO/IEC 27002.2005 controls ref 10.1.1 - 4, 10.3 & 12.1
- Data Protection Act 1998, Principle 7
- Data Protection Act 1998, Schedule 1, Part II, Paragraph 11

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**Responsibility has been assigned to a staff member for compiling information about the organisation's assets and for maintaining the asset register.**		
	a	Responsibility has been assigned for compiling and maintaining an information asset register. **Evidence Required:** • A named individual's job description, or a signed note or e-mail assigning responsibility.	❑
		Notes/other evidence:	
2	**A list of information assets has been compiled in a register which includes the location and 'owner' for each asset.**		
	a	All information assets have been documented in a register that includes relevant details about each asset (ie the location of each asset, what type of information, who uses it etc). **Evidence Required:** • Documented Information Asset register.	❑
		Notes/other evidence:	
3	**The asset register is maintained, reviewed and updated as necessary. Responsibilities and the asset register are regularly reviewed.**		
	a	The asset register is maintained, updated and regularly reviewed, eg to ensure that each asset is still required and is still in use or to add new assets to the register. **Evidence Required:** • Updates to the register or a date and signature indicating it has been reviewed.	❑
		Notes/other evidence:	
	b	[Level 3 Maintenance - only required if Level 3 achieved in previous year] It is important that the information asset owner carries out their responsibilities appropriately to ensure the currency of the register is maintained and that whenever new assets are introduced to the organisation the register is updated. **Evidence Required:** • Minutes/meeting notes where the responsibilities were reviewed during the year including the decisions made and any updates to the register.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

Unauthorised access to the premises, equipment, records and other assets is prevented	Requirement No:	11-317
	Initiative:	Information Security Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

It is important to ensure that the organisation's assets, premises, equipment, records and other assets including staff are protected by physical security measures.

Securing the Premises

Introduction

1. It is likely that there are well established procedures for premises security as a matter of course, often with sophisticated commercial asset and risk management procedures in place. Whilst the focus traditionally has been to safeguard medicines and staff, the NHS Information Governance requirements require procedures to safeguard the security of hardware, software and information.
2. Therefore there must be measures in place to delay and prevent unauthorised access, to detect attempted or actual unauthorised access, and to ensure that there are procedures for staff to follow in the event that unauthorised access does occur. The protection provided to premises should be balanced against the identified risks - that is, there should be an assessment of whether a particular risk is likely to occur and appropriate measures put in place to minimise that risk.

Security for Consultation Areas (including Pharmacy Dispensary)

3. Particular attention should be paid to the consultation and surgery areas. These are likely to contain patient or service user information on computers or in hard copy form. Paper copies of sensitive information should not be left unattended in the consultation/surgery area. Computer workstations in the consultation/surgery area, if left unattended, should be physically secured, and password protected when not in use.
4. The dispensary area should never be left completely unattended during the hours of business. Pharmacies should consider the minimum number of staff required to be in attendance in the dispensary given the floor-space of the premises, the time of day and any other risks. Consideration should be given to the physical security of paper records and computer workstations, relative to risk. If necessary, specialist guidance on security may be available from loss adjustment/commercial risk advisers.

Security for Office and Store Areas

5. A risk assessment should be undertaken on the security of offices and storerooms. Key considerations are the type of information stored in these areas, whether there is an adequate minimum staff level in these areas, and whether the rooms are in routine use. There may be a need to consider physical security measures such as keeping doors locked during working hours when the rooms are not in use.

Window Security

6. Windows in ground floor rooms are favourite access points for burglars and, particularly during hot weather, staff should ensure that they are closed when the room is not occupied. A risk assessment should be undertaken with possible physical security measures including window locks or if the area contains information or products which need to be particularly protected, window shutter systems or security grilles may be appropriate.

Back Doors and Fire Escapes

7. On some premises, back doors and fire escapes may be left ajar for ventilation purposes in hot weather. This practice has the potential to compromise the security of the premises and should be discouraged.

Alarms

8. There should be an alarm system that is of an adequate specification to protect the premises. Security specialists should be engaged when installing a new alarm system, or taking over new premises. Alarm systems should be tested on a regular basis. When refitting the premises, or developing new services, there should be consideration of whether the existing alarm system is adequate for the new security requirements, and seek security advice if necessary.

9. Fire alarms should be fitted in all areas and regularly tested. Fire doors, automatic and manually operated fire control systems all help prevent the spread of fire.

Keys and Staff Access

10. Physical keys should be issued on a need-to-have basis and a degree of inconvenience may be preferable to a large number of duplicate keys. Electronic keys can be cancelled with relative ease, but it can be time consuming and expensive to change locks on doors. A record should be kept of keys issued for long-term use and staff should be briefed on the importance of reporting lost keys. A log should be maintained, and procedures adopted to ensure keys have been returned when staff members have left employment.

Clear Desk and Clear Screen Policy

11. Staff should be encouraged to clear desks (including dispensing benches) of all sensitive and confidential information when it is no longer required for the task in hand and to ensure that such information is locked securely away over night. Staff should also be informed of how to use a password protected screen saver on their computers if they need to leave their machine unattended.

Assessment of Physical Security

12. There should be an assessment of physical security. This should look at the premises as a whole, taking into account legitimate entry and exit points, areas where forced entry is possible and any unstaffed parts of the building(s). Having identified any areas of risk, the risks should be weighed against the likelihood of the threatened risk actually occurring. For example, the assessment may identify a risk of burglary, the question to be asked is whether this a high risk, a medium risk or a low risk.

13. Where the risk of a breach in security is likely, the necessary resources should be allocated to increase the physical security of those assets. In the example above this may require installing security grilles on ground floor windows to minimise the risk of a break-in.

14. Where the perceived risk is low, it may be decided that action is unnecessary at this time; however, this should be documented and that area kept under regular review.

15. Physical security should be subject to regular risk assessment and updated guidance/ procedures issued to reflect new risks to the premises due to new ways of working or the purchase of new equipment. There should be checks that staff members comply with the procedures, eg by review of burglar alarm logs. Awareness and training should be provided to all new staff as part of their induction, and existing staff should be provided with regular updates as necessary.

Steps to Take Following Unauthorised Access

16. Measures should be put in place so that staff members are aware of the steps to take should unauthorised access occur, eg ensuring that they do not enter the premises alone where there is evidence of a break-in as the burglar may still be inside. There should also be advice about who to notify and minimising the losses where possible.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
DH: NHS IG - Information Risk Management - Good Practice Guide 2009	This guidance is aimed at those responsible for managing information risk within NHS organisations. It reflects government guidelines and is consistent with the Cabinet Office report on ‘Data Handling Procedures in Government’. This GPG also includes guidance on the need for Forensic Readiness Policy and local implementation.	24/01/2013

DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013
General Pharmaceutical Council: Conduct, Ethics and Performance	The Code of Ethics applies to both pharmacists and pharmacy technicians. It is published with supporting professional standards and guidance documents that have been developed to expand upon the principles of the Code for specific areas of practice or professional activities.	24/01/2013
College of Optometrists: Code of Ethics and Guidelines for Professional Conduct	The Code of Ethics is the basis of the whole professional conduct of optometrists, and all Fellows and Members of the College must subscribe to it.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Dental practice template: Physical Security Risk Assessment and Action Plan (XLS, 45 KB)	A spreadsheet to assist in carrying out a risk assessment of physical security developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
Dental practice template: Incident Reporting Form (DOC, 36 KB)	A template to enable the reporting of information governance incidents developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
Pharmacy template: Physical Security Risk Assessment Form (DOC, 87 KB)	A spreadsheet to assist in carrying out a risk assessment of physical security developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, the Department of Health and IG leads in the NHS.	24/01/2013

IG Resource Pack	These useful resources comprise staff awareness leaflets, exemplars, templates and model documents. Practices should scroll down the page for GP requirement specific resources.	24/01/2013
Surrey: Information Security and Confidentiality Guide for General Practice (DOC, 1366 KB)	This guide contains statements and guidance on Information Security and Confidentiality and is designed as both an informative guide and practical tool to guide the practice through the responsibilities of information security and confidentiality within a general practice.	24/01/2013
Cheshire: Adapted Risk Assessment Form for General Practice (DOC, 260 KB)	Form for assessing the risks to information, such as those posed by casual access, unauthorised access, mobile computing, disposal processes, and hazards of interrupted power supply, fire, water damage and other environmental hazards.	24/01/2013
Walton Centre: Access Authentication Standard (Physical) (PDF, 92 KB)	Standards and procedures that outline the way in which an organisation is able to prevent unauthorised access to assets physically.	24/01/2013
Voluntary Sector Template: YPAS Health and Safety Register (DOC, 71 KB)	Template Health and Safety register.	24/01/2013
Voluntary Sector Template: YPAS Health and Safety Checklist (DOCX, 45 KB)	Template Health and Safety Checklist	24/01/2013
Voluntary Sector Template: YPAS Risk Assessment Form (DOC, 52 KB)	Template risk assessment form.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of information risk management. Staff whose roles involve the handling of personal data will

benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.

- **NHS Information Risk Management** - a foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.
- **NHS Information Risk Management for SIROs and IAOs** - an introductory module that describes key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties. SIROs should also review the IRM Foundation module.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- Data Protection Act 1998, Principle 7
- Royal Pharmaceutical Society of Great Britain (RPSGB) Professional standards for pharmacists, PS 3 Pharmacy Premises and Facilities Standard 3.2
- College of Optometrists - Code of Ethics and Guidelines for Professional Conduct: A02- Patient Practitioner Relationship, A2.18 Premises
- Confidentiality and Disclosure of Information: General Medical Services (GMS), Personal Medical Services (PMS), AND Alternative Provider Medical Services (APMS) Code of Practice paragraph 17 (v).

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**A risk assessment of physical security of the premises has been carried out and staff members have been informed of steps to take in the event of unauthorised access.**		
	a	A risk assessment has been undertaken to identify areas of the premises that are at risk of unauthorised access. This covers the premises as a whole, and takes into account legitimate entry/exit points, areas where forced entry is possible and any unstaffed parts of the premises. **Evidence Required:** • A documented risk assessment including details of any required improvements.	❑
		Notes/other evidence:	
	b	There is a reporting process and safety measures in place for staff to follow in the event of unauthorised access. **Evidence Required:** • Documented staff guidance.	❑
		Notes/other evidence:	
2	**Improvements identified by the risk assessment are being made to secure the premises, equipment, records and other assets and staff.**		
	a	Improvements are being made to secure the premises, equipment, records and other assets. **Evidence Required:** • An action plan or allocation of resources or new security equipment (alarms, door locks, etc) or new ways of working (clear desk, clear screen, etc).	❑
		Notes/other evidence:	
	b	Staff members, including new staff, have been informed about new security measures put in place and the process for reporting unauthorised access through team meetings or awareness sessions or staff briefing or induction materials. **Evidence Required:** • Minutes/notes of team meetings, briefing and induction materials.	❑
		Notes/other evidence:	

3	**All reasonable steps have been taken to ensure the premises, equipment, records and other assets are physically secured. Physical security measures are subject to regular risk assessment.**		
	a	All improvements identified by the risk assessment have been fully implemented to prevent unauthorised access to the premises, equipment, records and other assets. **Evidence Required:** • New security equipment (alarms, door locks, etc) or new ways of working (clear desk, clear screen, etc).	❑
		Notes/other evidence:	
	b	Providing staff with guidance and procedures for protecting the premises, equipment, records and other assets does not provide sufficient assurance that the guidance and procedures have been understood and are being followed, therefore compliance spot checks and routine monitoring are conducted. **Evidence Required:** • Completed audit sheets or monitoring forms, or a report on the outcome of staff compliance checks (eg review of burglar alarm logs, clear desk procedure, whether windows and doors are locked).	❑
		Notes/other evidence:	
	c	[Level 3 Maintenance - only required if Level 3 achieved in previous year] It is important that physical security measures are subject to regular risk assessment and updated guidance or procedures are issued to reflect new risks due to new ways of working or the purchase of new equipment. **Evidence Required:** • Risk assessments will include checks that security measures are working effectively and that staff are complying with procedures.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions	Requirement No:	11-319
	Initiative:	Information Security Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.1

Requirement Description

In the event of a security failure or a disaster, natural, accidental or deliberate, vital business processes still need to be carried out. Having documented *business continuity plans* and procedures assists this process enabling all staff to know what they need to do in the event of a security failure or disaster.

Business Continuity Planning

Introduction

1. Business Continuity Plans (BCP) represent an attempt by organisations to predict, assess and counteract threats and risks that may lead to events that seriously disrupt or curtail all or part of their business functions. Business Continuity assessments analyse the probability of untoward events occurring, their likely impacts, determine what the organisation can do if they happen, and how the organisation systematically goes about recovering from these events.
2. Organisations are likely to require support from their *commissioning organisation* to put appropriate plans and procedures in place. A template is also available from the **Knowledge Base Resources**.

Purpose of Business Continuity Planning

3. Business continuity planning enables an organisation to:
    a. assess the risks of a security failure or disaster occurring;
    b. analyse the consequences to the running of the organisation if a security failure or disaster was to occur;
    c. plan measures to reduce the likelihood of a security failure or disaster occurring;
    d. plan measures to allow the organisation to continue to function if a security failure or disaster does occur.
4. A senior staff member should oversee risk assessments and coordinate an overall assessment plan for the organisation.

Critical Information Systems

5. Critical information systems should include all systems containing patient/service user data and communication systems necessary for transmitting patient/service

user information. Critical processes should include those necessary for delivering patient/service user care.

6. Risks to the confidentiality, integrity and availability of systems and processes should be assessed. The impact of threats should be assessed to determine priorities and plans put in place to counter the threats. Critical times (those affecting the potential to deliver adequate patient/service user care) should be assessed and countermeasures put in place to ensure system or process recovery occurs within agreed time limits.
7. Plans should be tested as table-top exercises and walk-throughs (such as validation of data back-ups).
8. Review groups should be established to take responsibility for review, coordination and testing of the plans. A regular review and testing timetable should be established, with both being conducted on an annual basis. Reviews should also be carried out following significant system changes, relocation of facilities and staff reorganisation.
9. An independent audit team, eg from the commissioning organisation, should be used to assess the ability of plans to meet their objectives.

Information Security and Business Continuity Planning Terminology

10. **Risk assessment:** Assessment of threats, impacts and vulnerabilities on organisational services and assets to enable measures to be taken to reduce the identified risks.
11. **Disaster:** Accidental, natural or malicious events, which threaten or disrupt normal operations or services for sufficient time to have significant effects on the organisation's business.
12. **Threat:** A potential cause of an unwanted incident, which may result in harm to a system or organisation.
13. **Confidentiality:** Ensuring that information is accessible only to those authorised to have access.
14. **Integrity:** Safeguarding the accuracy and completeness of data and information and processing methods.
15. **Availability:** Ensuring that authorised users have access to information and associated assets when required.

    Please note, it is best practice to ensure that any suppliers to the organisation also adhere to this requirement

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013
HSCIC: IG Serious Incidents Requiring Investigation Checklist Guidance (PDF, 204 KB)	This guidance document covers the reporting arrangements and describes the actions that need to be taken in terms of communication and follow up when an IG SIRI occurs. Organisations should ensure that any existing policies for dealing with IG SIRIs are updated to reflect these arrangements.	
DH: NHS IG - Information Risk Management - Good Practice Guide 2009	This guidance is aimed at those responsible for managing information risk within NHS organisations. It reflects government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures in Government'. This GPG also includes guidance on the need for Forensic Readiness Policy and local implementation.	24/01/2013
DH: Good Practice Guidelines - Destruction of Data and Media Containing Sensitive Data (PDF, 74 KB)	Guide to safely and securely destroying data and media containing confidential and sensitive information.	24/01/2013

Business Continuity Manual 2003 (PDF, 348 KB)	The purpose of this document is to give clear guidance to enable all organisations including strategic health authorities, special heath authorities, trusts and agencies to develop their own effective business continuity plans. It aims to provide a common basis and understanding for identifying key assets, assessing the risks and their impacts and following the development of those plans to test, implement and maintain them.	24/01/2013
HSCIC: Good Practice Guidelines in Information Governance - Information Security	The Good Practice Guidelines (GPG) are a series of informational documents which provide best practice advice in technology specific areas of Information Security.	24/01/2013
General Medical Council: Good Medical Practice	Good Medical Practice sets out the principles and values on which good practice is founded; these principles together describe medical professionalism in action. There are links to other GMC guidance and information which illustrate how the principles in Good Medical Practice apply in practice, and how they may be interpreted in other contexts.	24/01/2013
General Dental Council: Standards for Dental Professionals	The GDC produced and published its core guidance, Standards for Dental Professionals in 2005. This booklet, and the supplementary guidance booklets and statements which support it, lists the principles and values within which dental practitioners should operate.	24/01/2013
General Pharmaceutical Council: Conduct, Ethics and Performance	The Code of Ethics applies to both pharmacists and pharmacy technicians. It is published with supporting professional standards and guidance documents that have been developed to expand upon the principles of the Code for specific areas of practice or professional activities.	24/01/2013
College of Optometrists: Code of Ethics and Guidelines for Professional Conduct	The Code of Ethics is the basis of the whole professional conduct of optometrists, and all Fellows and Members of the College must subscribe to it.	24/01/2013

Joint IT Committee: The Good Practice Guidelines for GP electronic patient records Version 4 (2011) (PDF, 1732 KB)	The new Good Practice Guidelines for GP electronic patient records v4 (GPGv4 2011) will act as a reference source of information for all those involved in developing, deploying and using general practice IT systems.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Dental practice template: Business Impact Analysis Sheet (XLS, 31 KB)	A spreadsheet to assist in assessing the likely impact of loss of services in a dental practice, developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
Dental practice template: Emergency and Business Continuity Plan (DOC, 172 KB)	A template business continuity plan developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
DH: NHS IG - ISMS Risk Assessment Template 2008 (DOC, 43 KB)	This NHS IG template is provided to assist NHS organisations and General Practices to identify, assess and evaluate the treatment of risk that is appropriate to their local business needs.	24/01/2013
IG Resource Pack	These useful resources comprise staff awareness leaflets, exemplars, templates and model documents. Practices should scroll down the page for GP requirement specific resources.	24/01/2013
Bite-sized Good Practice Guide: Business Continuity (DOC, 287 KB)	IG Policy team leaflet on good practice in business continuity.	24/01/2013
Cheshire: Adapted Risk Assessment Form for General Practice (DOC, 260 KB)	Form for assessing the risks to information, such as those posed by casual access, unauthorised access, mobile computing, disposal processes, and hazards of interrupted power supply, fire, water damage and other environmental hazards.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Pharmaceutical Services Negotiating Committee: IG Web Pages	Information for community pharmacy on NHS Information Governance - the IG training booklet can be downloaded from this site.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of information risk management. Staff whose roles involve the handling of personal data will benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.
- **NHS Information Risk Management** - a foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.
- **NHS Information Risk Management for SIROs and IAOs** - an introductory module that describes key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties. SIROs should also review the IRM Foundation module.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- Data Protection Act 1998, Principle 7
- The National Health Service (General Dental Services Contracts) Regulations 2005, Part 5 section 40 - requirement to notify the PCT in writing of serious incidents
- The National Health Service (Personal Dental Services Agreements) Regulations 2005, Part 5, section 41 - requirement to notify the PCT in writing of serious incidents

- General Dental Council - Guidance on Principles of Management Responsibility, Your own behaviour 1.9
- General Dental Council - Guidance on Principles of Management Responsibility, The behaviour of other people in your organisation 2.5
- National Health Service England General Ophthalmic Services Contracts Regulations 2008, Part 4, section 16(1) - requirement to notify the PCT in writing of serious incidents
- College of Optometrists - Code of Ethics and Guidelines for Professional Conduct: A09 Patient records - A9.13 and A9.15
- Standard General Medical Services contract clauses 455 - 455.1 - requirement to notify the PCT in writing of serious incidents
- NHS Pharmaceutical Regulations 2005, schedule 1, Part 26(2)(c) a risk management programme

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**There has been an assessment of the risks to all systems where information critical to the running of the organisation is held.**		
	a	There has been an assessment of the risks to all systems where information critical to the running of the organisation is held which has been documented. **Evidence Required:** • A business impact analysis document.	❑
		Notes/other evidence:	
2	**There is a business continuity plan that has been approved by senior management. All staff are aware of their roles and responsibilities.**		
	a	There is an approved business continuity plan in place, which has been approved by senior management. **Evidence Required:** • Documented business continuity plan. • Approval may be in the minutes/notes of meetings, in a document or email or a personal endorsement in writing from an appropriately senior manager.	❑
		Notes/other evidence:	
	b	All relevant staff are made aware of the business continuity plan and any implications for their role. **Evidence Required:** • Notes/minutes from team meetings, or briefing materials used in awareness sessions.	❑
		Notes/other evidence:	
3	**There is an approved business continuity plan in place which has been tested. The business continuity plan is regularly reviewed.**		
	a	Annual testing is carried out to ensure that business continuity plans are effective and robust and will work in an operational environment. **Evidence Required:** • Documentation for testing processes (eg a table top exercise, simulation, or walk through exercise), or minutes/notes of discussions detailing agreed tests.	❑
		Notes/other evidence:	

	b	[Level 3 Maintenance - only required if Level 3 achieved in previous year] It is important that business continuity plans are regularly reviewed and updated (and in particular when new threats are identified) so that the organisation has the necessary assurances that plans are capable of being executed effectively. **Evidence Required:** • Minutes/meeting notes where the plan has been reviewed during the year including the decisions made and any updates to the plan.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

There are documented incident management and reporting procedures	Requirement No:	11-320
	Initiative:	Information Security Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

Information incidents include a loss of patient/service user data, a breach of confidentiality or other effect on the confidentiality, security or quality of patient/service user information. All incidents and near-misses should be reported, recorded and appropriately managed so that where incidents do occur, the damage from them is minimised and lessons are learnt from them.

Incident Management and Reporting

Introduction

1. Information incidents are any event or occurrence that has resulted or could have resulted in either the disclosure of confidential information to an unauthorised individual, put at risk the integrity of the system or data, or put at risk the availability of the system.
2. Under their terms of agreement, general practices are required to notify their service commissioners in writing of all serious incidents that affect or are likely to affect their contractual obligations. Whilst the commissioner will necessarily be concerned with clinical incidents, information incidents should not be overlooked as they can also have a serious affect on patient care. Other NHS contractors should also consider whether it is appropriate to inform service commissioners or other external organisations of Serious Incidents Requiring Investigation (SIRIs), for example if this is likely to lead to a patient complaint.
3. Voluntary/third sector organisations should also have processes in place to notify information incidents to the organisation or individual that has commissioned them to provide services.
4. In the case of person identifiable information provided to a recipient organisation for secondary uses, eg a transfer of patient data approved under Section 251 of the NHS Act 2006, robust arrangements must be in place to ensure that the data provider or sponsoring organisation or statutory body is notified of all information incidents.
5. An IG SIRI is any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 1998 and/or the Common Law of Confidentiality. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy. This definition applies irrespective of the

media involved and includes both electronic media and paper records. Further detail on the current process, assessing the severity of incidents, severity levels which are reported to national Bodies etc. can be found within the latest **'Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation'** (See Knowledge Base Resources). Local clinical and corporate incident management and reporting tools can continue to be used for local purposes but notifications of IG SIRIS for the attention of DH and the ICO must be communicated using the IG Incident Reporting Tool with immediate effect.

6. From June 2013 all Organisations processing health and social care personal data are required to use the IG Toolkit Incident Reporting Tool to report level 2 IG Serious Incidents Requiring Investigation (SIRI) to the Department of Health, NHS England and Information Commissioner's Office.

Identifying an Information Incident

7. Information incidents are not always apparent. For example, a computer stolen during a burglary may be seen as merely a hardware issue. However, the information contained on the computer, especially sensitive information, can undermine the security and good reputation of the organisation, if disclosed to those not authorised to see it. Other incidents should also be taken into account, eg an attempt to access confidential information by an unauthorised person; a software malfunction; etc.

Managing Information Incidents

8. There has been a requirement to record and analyse critical incidents in relation to medicines for some time. The underlying principles are equally applicable to the management of information incidents. These include:

    a. establishing that an incident has, in fact, occurred;

    b. establishing where the responsibility for the incident lies;

    c. evaluating the extent of the damage or risk to the organisation as a result of the incident;

    d. taking timely and appropriate remedial action;

    e. reviewing procedures to reduce the risk of the incident occurring again, and keeping a record of lessons learned.

9. Responsibility should be assigned for managing information incidents to an appropriate member of staff and procedures put in place for the reporting and management of incidents. In small organisations this responsibility may reside with the IG Lead.

10. The incident management procedures should detail:

    a. the need for the procedure;

    b. the scope of the procedure;

    c. a brief explanation of the types of incident, how they will be managed and reported and any countermeasures;

    d. responsibilities of management and staff towards incident reporting;

e. referenced documentation (eg the Information Governance policy);

f. current NHS and national guidelines (eg NHS incident reporting for viruses).

g. If appropriate, If you experience any issues with your system/service, please log this directly with your system supplier.

h. how to report SIRIs using the IG toolkit Incident Reporting Tool to inform Department of Health, NHS England and Information Commissioner's Office.

11. Some of the procedures will be discrete, such as investigating computer misuse (child pornography, fraud) and others will form part of *Business Continuity Plans*, eg in the event of complete computer failure, see also **requirement 319**.

12. The procedures should include a process of review to allow discussion and reflection in the event of an incident. The review should involve all disciplines of staff and the process should be carried out avoiding the allocation of blame. A culture of blame is not conducive to improvements being made; lessons can usually be learnt from any identified shortcomings allowing improved processes for the future. Where applicable, new countermeasures and procedures should be put in place to avoid a repetition of the event.

Recording Information Incidents

13. All information should be recorded on the IG Toolkit Information Reporting Tool:

a. date of incident (if identifiable);

b. location of incident (if identifiable);

c. details of staff involved (if identifiable and applicable);

d. description of incident;

e. degree of risk associated with the incident (correlates with risk assessment for data transfer) - see **requirement 322**;

f. any contributing factors;

g. remedial action taken following this incident;

h. suggested action to be taken to prevent a reoccurrence of this incident;

i. informing the insurer and others (if appropriate), eg the police, the *Information Commissioner's Office* and the commissioning organisation.

Reporting Information Incidents

14. It is essential that all staff members are aware of the necessity to report information incidents, including lost or stolen equipment, breaches of confidentiality and near-misses.

15. Staff should be fully informed and trained in the use of all procedures in place to protect information. No matter how good existing procedures are weaknesses will always become apparent. New threats and new systems or ways of working will expose these weaknesses and users on the ground are normally the first to identify them. Therefore, staff should be encouraged to report anything they feel threatens security. This approach needs to be adopted during induction training.

16. If there is a standard reporting form it should also include information incident reports. All incident reports should be referred for further action to the person assigned responsibility for managing information incidents.

17. The person who has responsibility for managing information incidents should consider whether it is appropriate to inform the commissioning organisation of high risk incidents, for example if this is likely to lead to a patient/service user complaint. It is also considered best practice to inform the Information Commissioner if the data loss falls into a high risk category, the IG Toolkit Incident Reporting Tool does this for you as part of an automated notification process. It may be appropriate to report the incident to others including the police, for example in the event of data theft, or to the insurer, eg in the case of stolen equipment.

    Please note - it is best practice to ensure that any suppliers to the organisation aldo adhere to this requirement.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
HSCIC: IG Serious Incidents Requiring Investigation Checklist Guidance (PDF, 204 KB)	This guidance document covers the reporting arrangements and describes the actions that need to be taken in terms of communication and follow up when an IG SIRI occurs. Organisations should ensure that any existing policies for dealing with IG SIRIs are updated to reflect these arrangements.	
HSCIC: IG Serious Incidents Requiring Investigation Reporting Tool Publication Statement (PDF, 61 KB)	The purpose of this statement is to inform IG Toolkit Users and members of the public of our intent to publish data on Serious Incidents Requiring Investigation (IG SIRI) self reported on the secure IG Toolkit Information Governance (IG) Incident Reporting Tool.	
DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013

DH: NHS IG - Information Risk Management - Good Practice Guide 2009	This guidance is aimed at those responsible for managing information risk within NHS organisations. It reflects government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures in Government'. This GPG also includes guidance on the need for Forensic Readiness Policy and local implementation.	24/01/2013
General Dental Council: Standards for Dental Professionals	The GDC produced and published its core guidance, Standards for Dental Professionals in 2005. This booklet, and the supplementary guidance booklets and statements which support it, lists the principles and values within which dental practitioners should operate.	24/01/2013
General Pharmaceutical Council: Conduct, Ethics and Performance	The Code of Ethics applies to both pharmacists and pharmacy technicians. It is published with supporting professional standards and guidance documents that have been developed to expand upon the principles of the Code for specific areas of practice or professional activities.	24/01/2013
College of Optometrists: Code of Ethics and Guidelines for Professional Conduct	The Code of Ethics is the basis of the whole professional conduct of optometrists, and all Fellows and Members of the College must subscribe to it.	24/01/2013
Joint IT Committee: The Good Practice Guidelines for GP electronic patient records Version 4 (2011) (PDF, 1732 KB)	The new Good Practice Guidelines for GP electronic patient records v4 (GPGv4 2011) will act as a reference source of information for all those involved in developing, deploying and using general practice IT systems.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Dental practice template: Incident Management Procedures (DOC, 67 KB)	Template incident management procedures developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013

Dental practice template: Incident Register (DOC, 47 KB)	A template to enable the recording of information governance incidents developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
Dental practice template: Incident Reporting Form (DOC, 36 KB)	A template to enable the reporting of information governance incidents developed for dental practices by the British Dental Association, the Department of Health, and IG leads in the NHS.	24/01/2013
Pharmacy template: Information Security Incident Management Procedure (DOC, 48 KB)	Template incident management procedures developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, the Department of Health and IG leads in the NHS.	24/01/2013
Pharmacy template: Information Security Incident Report Form (DOC, 44 KB)	A template to enable the reporting of information governance incidents developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, the Department of Health and IG leads in the NHS.	24/01/2013
Pharmacy template: Staff Signature List (DOC, 45 KB)	A template for staff to sign to confirm their understanding of the responsibilities they carry for the proper handling of confidential patient information. Developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, the Department of Health and IG leads in the NHS.	24/01/2013
Pharmacy template: Staff Signature List (Separate Lists) (DOC, 213 KB)	A template for staff to sign to confirm their understanding of the responsibilities they carry for the proper handling of confidential patient information. Developed for the community pharmacy setting by the Pharmaceutical Services Negotiating Committee, the Royal Pharmaceutical Society of Great Britain, DH and IG leads in the NHS.	24/01/2013

IG Resource Pack	These useful resources comprise staff awareness leaflets, exemplars, templates and model documents. Practices should scroll down the page for GP requirement specific resources.	24/01/2013
Cheshire: Handling Security Incidents Affecting Patients Confidentiality (DOC, 66 KB)	This guidance suggests mechanisms for handling security incidents where patient confidentiality has been or may have been breached.	24/01/2013
East Surrey: Incident Reporting Policy 2002 (DOC, 66 KB)	The document details a process for identifying, recording and monitoring non-clinical incidents.	24/01/2013
Walton Centre: Incident Reporting Standard (PDF, 182 KB)	This standard covers two separate but closely related areas: incident reporting, and incident response. Incident management is a cyclical process that requires identification/reporting of incidents, investigations and resolution and learning to reduce the risk of recurrence.	24/01/2013
Walton Centre: Incident Response Standard (Legal and Forensics) (PDF, 192 KB)	A detailed incident response process including steps to take if legal and/or forensic expertise is required.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
ISO/IEC TR 18044:2004 - Information Security Incident Management	This Technical Report (TR) provides advice and guidance on information security incident management for information security managers, and information system, service and network managers. Available to purchase from the British Standards Institute website.	24/01/2013
ITIL: The IT Infrastructure Library	The ITIL series of publications is designed to provide advice on how to prepare and deal with IT related management problems. The publications are available to purchase from the TSO online bookshop.	24/01/2013

Pharmaceutical Services Negotiating Committee: IG Web Pages	Information for community pharmacy on NHS Information Governance - the IG training booklet can be downloaded from this site.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of information risk management. Staff whose roles involve the handling of personal data will benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.
- **NHS Information Risk Management** - a foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.
- **NHS Information Risk Management for SIROs and IAOs** - an introductory module that describes key responsibilities for the SIRO and IAO roles, and outlines the structures required within organisations to support those staff with SIRO or IAO duties. SIROs should also review the IRM Foundation module.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.
- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- The National Health Service (General Dental Services Contracts) Regulations 2005, Part 5 section 40 - requirement to notify the PCT in writing of serious incidents
- The National Health Service (Personal Dental Services Agreements) Regulations 2005, Part 5, section 41 - requirement to notify the PCT in writing of serious incidents
- General Dental Council - Guidance on Principles of Management Responsibility, Your own behaviour 1.9
- General Dental Council - Guidance on Principles of Management Responsibility, The behaviour of other people in your organisation 2.5

- National Health Service England General Ophthalmic Services Contracts Regulations 2008, Part 4, section 16(1) - requirement to notify the PCT in writing of serious incidents
- Standard General Medical Services contract clauses 455 - 455.1 - requirement to notify the PCT in writing of serious incidents
- Quality and Outcomes framework organisational domain – education and training indicators.
- Data Protection Act 1998, Principle 7
- NHS Pharmaceutical Regulations 2005, Schedule 1, Part 4, s26(2)(c) (iii) - an approved incident reporting system
- Royal Pharmaceutical Society of Great Britain (RPSGB) Professional standards and guidance for pharmacists, PS 2 Policies and Procedures Standard; PS 7 Enabling others to raise concerns

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**Responsibility for leading on the management and reporting of information incidents has been assigned to an appropriate member of staff.**		
	a	Responsibility for leading on the management and reporting of information incidents has been assigned to an appropriate member of staff. Where necessary and available, support is obtained from the commissioning organisation. **Evidence Required:** • A named individual's job description, or a signed note or e-mail assigning responsibility. • Evidence of commissioning organisation support if required may be in email communications, or in a formal SLA.	❑
		Notes/other evidence:	
2	**Incident management and reporting procedures have been implemented and staff have been informed of how to report incidents and near-misses.**		
	a	There are incident management and reporting procedures. **Evidence Required:** • Documented procedures and a template incident reporting form for staff.	❑
		Notes/other evidence:	
	b	Staff members have been informed of the incident reporting procedures and in particular of their own responsibilities for reporting incidents and near-misses. **Evidence Required:** • Minutes/notes of team meetings, or briefing materials used in awareness sessions.	❑
		Notes/other evidence:	
	c	Any information incidents that arise are reported to the senior management team and where necessary to the commissioning organisation and external parties. Reports include details of investigations or action taken and detail any possible countermeasures. **Evidence Required:** • Completed incident reporting forms and reports made to senior management and where necessary to the commissioning organisation, the Information Commissioner, insurers, or the police.	❑
		Notes/other evidence:	

3	**Incident reporting and management procedures are being followed and appropriate action is taken in the event of an incident or near-miss. Incident reporting and management procedures are regularly reviewed.**		
	a	Providing staff with procedures for reporting incidents does not provide sufficient assurance that the procedures have been understood and are being followed. Therefore compliance checks and routine monitoring are conducted. **Evidence Required:** • A completed audit sheet or monitoring form, or a report on the outcome of staff compliance checks.	❑
		Notes/other evidence:	
	b	Information incidents and near-misses are appropriately discussed with staff and where necessary, retraining is carried out or new security measures are implemented. **Evidence Required:** • Minutes/meeting notes or lessons learned documents. Where necessary, training materials or evidence of new measures put in place.	❑
		Notes/other evidence:	
	c	[Level 3 Maintenance - only required if Level 3 achieved in previous year] No matter how good existing procedures are weaknesses will always become apparent. New threats and new systems or ways of working will expose these weaknesses and users on the ground are normally the first to identify them. Therefore, staff should be encouraged to report anything they feel threatens security, and this approach needs to be adopted during induction training. **Evidence Required:** • Staff briefing materials, or incident report forms, or induction materials or new security measures.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	

All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures	Requirement No:	11-323
	Initiative:	Information Security Assurance
	Organisation Type:	Commercial Third Party
	Version:	11.0

Requirement Description

Organisations must ensure that all of their *information assets* that hold or are *personal data* are protected by technical and organisational measures appropriate to the nature of the asset and the sensitivity of the data.

Protection of Information Assets

Introduction

1. All organisations own and use information assets that support their local business needs (see **requirement 307** or **316** dependent on organisation-type). A subset of these assets will be personal data in some form and/or the equipment within which personal data is held. The majority of these information assets will underpin service user / patient care processes, human resource processes, activity management or clinical audit, research or service evaluation but there may be a wide range of other business activities supported by such assets. Whilst all information assets should be protected the importance of ensuring that this particular subset is held securely is paramount.

Examples of information assets relevant to this requirement	
• Paper records (service user, patient records and staff records) • Other media records (audio, images, scans etc) • Paper reports (clinical, research, service evaluation, complaints, waiting times)	• Computing hardware including PCs • Blackberry and removable media • Smartphones • Tablet computers • Databases and data files • Back-up and archive data • Audit trail data

Responsibilities

2. An *Information Asset Owner* (IAO), or equivalent, should be assigned unique responsibility for each significant information asset, or group of assets, of the organisation. For example, a Director of IM&T may be the IAO for network servers, desktop computers, laptops and other IT equipment.

3. It is essential that each IAO understands the scope and boundaries of their assigned information assets, their approved purposes, who the users of the assets are and what their requirements for guidance and training may be, the criticality of the assets to the organisation, their dependency on other assets, and which other assets are dependent upon them. In order to achieve this detailed understanding, it is necessary that each information asset and its component parts are identified within an asset register or inventory that allows the Information Governance safeguards to be considered individually and collectively.

4. Safeguards fall into two categories:

    a. those mandated for the public sector;

    b. those that might be deployed to mitigate against risks.

Safeguards mandated for the public sector

5. These safeguards include:

    a. Servers should be kept in a physically secure area inaccessible to unauthorised individuals or an *encryption* solution must be deployed. Encryption is recommended in all cases.

    b. An encryption solution must be deployed to protect all laptops, computer discs, memory sticks, back-ups and other removable or portable media in line with mandatory requirements and standards.

    c. *Anti-virus* software should be installed on each computer and configured to check all possible sources of infection eg CD and DVD-ROMs, USB devices, email, websites, downloaded files etc. The anti-virus software should be kept up to date at all times.

    d. The operating systems of computers should be regularly updated with published security patches.

    e. Drives and ports etc that are unnecessary for the business purposes should be disabled.

    f. The disposal or destruction of information assets must be managed securely following agreed procedures.

    g. There must be clearly defined and manageable rules for access and use of the information asset based on the need to know principle.

Safeguards that might be deployed to mitigate against risks

6. These safeguards include:

    a. **Anti-theft measures**: Have desktop and laptop computers used in public areas been equipped with anti-theft devices?

    b. **Premises security**: Have staff been assigned responsibility for locking doors and windows in locations where an information asset is located? What are the controls for storing assets (eg lockable cabinets), and are they used appropriately by staff?

    c. **System classification**: Has there been an assessment of the business importance and sensitivity of information to be processed by the information asset and has a classification been assigned to the system and/or its data?

d. **Backups**: Are procedures available to perform and test regular data backups, and is at least one copy of that data stored in a secure off-site location?

e. **Business continuity**: Is there a *business continuity plan* available and tested in case of a disaster?

NHS Websites

7. The security of NHS websites has a particular importance and visibility given the intended access to and use of these assets via the internet and/or the *NHS network* (N3). When assessing the security protection needs of an NHS website it is important that the risks to the website, including potential impacts to the organisation, its patients and other business disruptions are considered. Such risks can include the effects of hacking, defacement, content alteration and *denial of service*.

8. It is essential therefore that appropriate steps are taken to manage these risks and assure the website asset, irrespective of whether the website is designed, implemented and managed locally or delivered and maintained under agreement or contract by another party. All NHS organisations that possess or that are planning for websites must therefore have clearly defined procedures for the secure operation of each website, including procedures for their configuration patch and content management, business continuity and for dealing with incidents should they occur. In addition, organisations must take appropriate steps to ensure that the web server is not exposed to known vulnerabilities, eg by ensuring a regular healthcheck review and *penetration test* is made by a qualified tester. Records of tests should be made and improvement plans determined where necessary.

   Reference materials can found within the **Knowledge Base Resources**.

Additional Guidance: Secure Disposal or Re-Use of Equipment

9. Using computer utilities it is technically possible to retrieve data that has been 'deleted' from hard drives, removable disks and other media, eg digital photocopiers. Software to do this is available on the Internet and is relatively easy to use. Therefore, it is essential that classified or sensitive information (especially service user or patient data) is properly protected and securely disposed of when it is no longer required. This is also the case even where discs or media have been encrypted. Secure emergency recovery processes should be established where encryption has been used to encrypt files and discs. Such recovery processes must only be available to properly authorised and trained staff and in accordance with approved procedures.

10. In the case of hard drives and removable media, disposal may mean physical destruction, if they are not being re-used within the organisation. Older equipment with hard drives that potentially contain data of the organisation are sometimes passed on to charities or disposed of by third parties. It is essential that equipment with hard discs or removable media, including USB connectable memory devices, that has processed classified or sensitive information is not passed on without first guaranteeing that all such data has been irrevocably destroyed. In the case of third party secure disposal, a written contract must enforce this requirement.

11. Backup media that have reached their ‘use by date’ or that are redundant should be physically destroyed beyond any further use by incineration, shredding or cutting.

12. IAOs should ensure that the IT Department and other departments that supply and maintain information processing equipment as components of their asset have relevant and approved procedures for the secure disposal of equipment that is no longer needed.

13. Where an internal department of the organisation is responsible for secure disposal services, they should keep a full auditable record of the details of the device or drive involved, the materials destroyed and what destruction method was used. Similarly if a specialist third party is used a full record must be kept along with the certificate of disposal / destruction provided by the third party.

    Please note - it is best practice to ensure that any suppliers to the organisation also adhere to this requirement.

Knowledge Base Resources

Key Guidance		
Title	**Details**	**Last Reviewed Date**
DH: Information Security NHS Code of Practice 2007	The Code is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice and replaces HSG 1996/15 – NHS Information Management and Technology Security Manual.	24/01/2013
DH: NHS IG - Information Risk Management - Good Practice Guide 2009	This guidance is aimed at those responsible for managing information risk within NHS organisations. It reflects government guidelines and is consistent with the Cabinet Office report on 'Data Handling Procedures in Government'. This GPG also includes guidance on the need for Forensic Readiness Policy and local implementation.	24/01/2013
DH: NHS IG - Guidance for the Classification Marking of NHS Information 2009 (PDF, 115 KB)	This NHS guidance is provided as good practice for NHS organisations of all types to consider in marking the records for which they are responsible.	24/01/2013
HSCIC: Good Practice Guidelines - Application Security	This guide covers various general user applications and their security.	24/01/2013

HSCIC: Good Practice Guidelines - Disposal and Destruction of Sensitive Data	This document aims to establish vendor and product independent guidelines to assist organisations in minimising the risks of data disclosure through inappropriate deletion of data, or inadequate destruction of media prior to disposal.	24/01/2013
HSCIC: Good Practice Guidelines - Web Server Security (PDF, 32 KB)	When setting up a web server, there are a number of good practices in relation to securing such servers which should be followed. The list provided should not be considered exhaustive but as a starting point for securing such servers.	24/01/2013
HSCIC: Good Practice Guidelines - Securing Web Infrastructure and Supporting Services	The purpose of this document is to provide information on good security practices in relation to the security, and securing, of Web infrastructure and associated systems. Securing Web Infrastructure and supporting services	24/01/2013
BS ISO/IEC 27000 Series of Information Security Standards	Note that only NHS Information Governance Toolkit (IGT) administrators may download a copy of the standards for use by their organisation. The administrator must be logged on to download these standards.	24/01/2013
BS ISO/IEC 20000-2:2005 Information Technology Service Management Code of Practice	The Code offers assistance to service providers planning service improvements or to be audited against BS ISO/IEC 20000-1:2005 and can be purchased from the BSI website.	24/01/2013

Exemplar Materials		
Title	**Details**	**Last Reviewed Date**
Walton Centre: Change Control Standard (PDF, 141 KB)	An operational change control process covering change initiation of change, control of change, record keeping, and decision making for all aspects of change on the Trusts information systems on computer.	24/01/2013
Walton Centre: Full Information Security Management System (DOC, 35 KB)	Walton Centre For Neurology & Neurosurgery NHS Trust - Full Information Security Management System.	24/01/2013

DHID: AQP Template - Information Asset Register (DOC, 78 KB)	A template to enable the recording of information assets.	24/01/2013

Useful Websites		
Title	**Details**	**Last Reviewed Date**
Cabinet Office: Best Management Practice Portfolio	Best Management Practice products present flexible, practical and effective guidance, drawn from a range of the most successful global business experiences. Distilled to its essential elements, the guidance can then be applied to every sort of business and organisation.	24/01/2013
ITIL: The IT Infrastructure Library	The ITIL series of publications is designed to provide advice on how to prepare and deal with IT related management problems. The publications are available to purchase from the TSO online bookshop.	24/01/2013

Training

The External Information Governance Delivery team within the Health and Social Care Information Centre has developed an Information Governance Training Tool (IGTT).

The following modules are relevant to this Requirement:

- **NHS Information Risk Management** - an introductory level module that is intended to provide an overview of the key elements of information risk management. Staff whose roles involve the handling of personal data will benefit from a greater understanding of Information Risk Management principles, and an insight into how these principles relate to their own roles.
- **NHS Information Risk Management** - a foundation level module intended to assist staff whose roles involve responsibility for the confidentiality, security and availability of information assets, in understanding and fulfilling their duties.
- **Business Continuity Management** - a foundation level module aimed at newly appointed staff and those needing to know a little more about the role of BCM.

As well as the interactive e-learning the tool has several other features, including:

- **Certificate** - on successful completion of an assessment.
- **Resource Library** - further reading documents and links to useful websites.
- **Trainer materials** - made up of PowerPoint presentations, tutor notes and audio clips.

- **Reporting function** - for the Department of Health and organisation administrators.

The Tool is available at: www.connectingforhealth.nhs.uk/igtrainingtool.

Requirement Origins

- ISO/IEC 27002.2005 controls ref 7, 9, 10.3 & 12.1
- Data Protection Act 1998, Principle 7
- Data Protection Act 1998, Schedule 1, Part II, Paragraph 9-12

Changes

There are no *material* changes since the last major version of this requirement.

Attainment Levels (Including Checklist)

These are cumulative eg to attain Level 3 you must complete all Level 1, 2 and 3 criteria.

0	**There is insufficient evidence to attain Level 1.**		❑
1	**There is an Information Asset Register that includes all assets that comprise or hold personal data, with a clearly identified accountable individual (IAO).**		
	a	There is an Information Asset Register that captures all identified information assets that comprise or hold personal data and there is a clearly identified individual accountable for each asset recorded in the Register. **Evidence Required:** • Documented Information Asset register.	❑
		Notes/other evidence:	
	b	A documented plan has been developed to investigate and identify all remaining information assets that comprise or hold personal data and to assign appropriate responsibility for any identified, including details in the Information Asset Register. **Evidence Required:** • Documented action plan.	❑
		Notes/other evidence:	
2	**All mandatory safeguards are in place to protect assets that comprise or hold personal data and risk assessments have been conducted to determine which additional safeguards should be in place.**		
	a	All mandatory safeguards are in place to protect identified assets that comprise or hold personal data. **Evidence Required:** • A clear description of the safeguards that have been deployed included within the Information Asset Register.	❑
		Notes/other evidence:	
	b	Risk assessments have been conducted to determine which, if any, additional safeguards should be deployed to protect each asset. **Evidence Required:** • A documented risk review report and any additional safeguards included in the Information Asset Register.	❑
		Notes/other evidence:	

	c	The plan to identify any relevant information assets that the organisation was previously unaware of has been implemented and there is a high degree of confidence that all such assets have been identified and secured. **Evidence Required:** • A documented report to an appropriate senior manager or committee.	❑
		Notes/other evidence:	
3	**All information assets that comprise or hold personal data have been effectively secured and audit/spot checks are used to check compliance.**		
	a	All information assets that comprise or hold personal data have been effectively secured and audit/spot checks are used to check compliance. **Evidence Required:** • Audit or spot check reports along with a documented schedule of checks that demonstrates that checks are made across the organisation.	❑
		Notes/other evidence:	
	b	All new information assets that comprise or contain personal data are identified when they are created/deployed and steps taken to include them in the Information Asset Register and to secure the data. **Evidence Required:** • A documented instruction to all Information Asset Owners or equivalent and the notes of a meeting where this was discussed/reviewed and agreed to be working effectively.	❑
		Notes/other evidence:	
	c	[Level 3 Maintenance - only required if Level 3 achieved in previous year] Requirements may change over time and new technical safeguards or working practices may be identified. **Evidence Required:** • Minutes/meeting notes of a review meeting where these matters were considered. • Audit or spot check reports along with a documented schedule of checks that demonstrates that checks are made across the organisation.	❑
		Notes/other evidence:	

Past Level: (available online from IGT)		**Current Level:**		**Target Level:**	
				Target Date:	