NHS Information Governance:

Effective Management of Records during a period of transition or organisational change

Information Governance Policy

Department of Health Informatics Directorate

September 2011

DH INFORMATION READER BOX

Policy	Estates
HR / Workforce	Commissioning
Management	IM & T
Planning /	Finance
Clinical	Social Care / Partnership Working

Document Purpose	Best Practice Guidance
Gateway Reference	16642
Title	NHS Information Governance: Effective Management of Records During a period of Transition or Organisational Change
Author	DH/Informatics/Information Governance Policy Branch
Publication Date	September 2011
Target Audience	PCT CEs, NHS Trust CEs, SHA CEs, Care Trust CEs, Foundation Trust CEs , PCT Chairs, Caldicott Guardians, Senior Information Risk Officers(SIROs)
Circulation List	Directors of HR, Directors of Finance, Communications Leads
Description	This document provides guidance on records management for NHS organisations who are going through a period of transition.
Cross Ref	Records Management: NHS Code of Practice
Superseded Docs	N/A
Action Required	Best practice
Timing	**N/A**
Contact Details	Catherinekay@nhs.net david.martin@dh.gsi.gov.uk
For Recipient's Use	

Contents

Glossary

Record	Anything which contains information (in any media) that has been created or gathered as a result of any aspect of the work of NHS employees, excluding trivial and/or transitory messages that are not subject to retention policies.
Health Record	A record which has been created by, or on behalf of, a health professional in connection with the care of an individual and which contains information about the physical or mental health of that individual.
Personal Information	Information which relates to an individual who can be identified by that information, or that information together with other information that may be available to the holder.
Processing	Any action which may take place on personal information including, but not limited to, storing, using, transferring or destroying of the information.
Data Controller	A person or organisation (either alone or jointly or in common with other persons) that determines the purpose for which, and the manner in which, any personal data is, or may be, processed. The fact that an individual or organisation holds or processes personal data does not make them a data controller, if they do not determine the purpose and manner of that holding or processing.
Data Processor	A person or body who processes information on behalf of a data controller but does not determine the purpose of that processing.
Archival	Storage of records which are to be retained but are no longer necessary for day-to-day use.
Active records	Records which relate to an activity which is still currently ongoing. This will normally mean that these records will or may be added to.
Inactive records	Records which relate to an activity which has now ceased. This will normally mean that these records are no longer being added to but are still currently held.

Introduction

As Strategic Health Authorities (SHA) and Primary Care Trusts (PCT) enter a period of transition it is essential that steps are taken to ensure that records are managed appropriately.

Records are associated with functions. It is important that service changes are managed carefully to ensure that the functions which are to continue can do so safely and efficiently. Functions which will not continue must also be managed carefully to ensure that legal obligations are met, valuable knowledge retained and historically valuable data preserved. This is not a trivial undertaking. It will require planning and attention to detail and may require difficult decisions.

This guidance provides detailed guidance for organisations going through transition. Further guidance about records management in general can be found in the Records Management: NHS Code of Practice and those with responsibility for records and information/knowledge management should ensure that they are familiar with the principles covered within the Code.

Responsibilities

Organisations will retain legal responsibility for the information that they hold until they are formally dissolved or until agreements are put in place to transfer responsibility. Organisations must make decisions about their records before they close. It is therefore important that organisations which are closing dedicate sufficient resource to the information management activities associated with the closure. Senior management awareness, involvement and support are essential and should be sought as soon as possible once planning begins. This may already be covered or could be done through an existing senior management/Trust Board transition group (or equivalent). All collections of information and records should have been captured in the organisation's information asset register – which should be updated if necessary – and all decisions about disposal or transfer should be recorded in this register.

Where functions are transferring to another organisation related records will normally be transferred too. In this situation responsibility, liability and accountability for records should also transfer and where there is no defined legislative basis transferring functions, organisations should draft agreements to clearly outline the terms of the transfer. Organisations must be clear who will have responsibility for handling Freedom of Information Act 2000 (FOI) and Data Protection Act 1998 Subject Access requests when information is to be transferred or functions move.

The transferring organisation has a responsibility to ensure that there are appropriate governance structures in place in the receiving organisation(s) before they transfer any information. The receiving organisation should, as a minimum, have assigned Senior Information Risk Owner responsibilities, have an information governance lead (or equivalent), and have a documented Information Governance Framework. All organisations that process personal information relating to NHS service users or staff should also be completing and publishing an annual IG Toolkit assessment and should have assigned Caldicott Guardian responsibilities. The IG Toolkit [1] provides very clear guidance on information governance requirements and on the roles and responsibilities that need to be covered

[1] The Information Governance Toolkit can be found at www.igt.connectingforhealth.nhs.uk

All organisations involved in the transfer of functions should make sure that they are fully aware of their responsibilities under the Public Records Act 1958. NHS organisations have a duty to transfer records that may have archival value to an appointed Place of Deposit for retention under s. 3(1) of that Act. This is likely to be particularly relevant in disposing of existing backlogs of records from previous re-organisations held in contract storage, or records relating to functions which have no obvious single successor. Place of Deposit representatives should be consulted early in the planning stages with regard to their potential role in the transfer of records.

Planning

As soon as is practicable organizations will wish to develop an action plan[2] to outline procedures for destruction, transfer or archival of information. Early planning will help organisations to manage the risks arising during transitions and allow them to:

- identify potential issues at an early stage;
- utilise existing expertise within the organisation;
- understand the resources available to carry out transition related work;
- seek legal and good practice advice where necessary;
- check that Data Protection notification/registration is updated to reflect any new or changed functions;
- identify what information needs to be shared and with whom;
- minimise the impact on those functions which are to transfer, and
- liaise and negotiate with receiving organisations, archives and government bodies.

Management

An Information Transition Group should be formed to steer the transition process. The group should include members with expert skills (e.g. information governance, data protection, records management, information security) relevant to issues arising during transition and members from both the closing and receiving organisations where applicable, to oversee and advise on the whole transition.

The Group should be the focal point for all issues arising in relation to records during transition and should be visible to staff in all departments to allow them to raise specific issues. In some cases it may be more appropriate for an existing transition management group (or equivalent) to take responsibility for managing records during the transition.

The Group should be managing a risk register linked into the corporate risk register. Where information or records are to be transferred to another body these links should be into the corporate risk registers of both the transferring and receiving bodies to ensure all risks are identified, managed and appropriate actions taken.

[2] An example action plan be found in The National Archives guidance 'What to do with your records if your public body is being dissolved' http://www.nationalarchives.gov.uk/documents/information-management/dissolution-of-public-bodies.pdf

Creating a Transitional Information Inventory

In order to effectively manage transition, organisations should produce an information inventory[3] outlining details about the information they hold and how they will handle this information through the transition. Organisations that have already mapped their information flows and have developed a comprehensive information asset register will be better placed to do this and these should form the basis of this exercise (refer to requirements 9-308 and 9-604 of the Information Governance Toolkit for further information). Inventories should contain details about:

- which records are currently held;
- where these records are;
- whether the records are currently active;
- the format records are held in and the equipment needed to read them;
- the appropriate department or contacts with responsibility for the records;
- how old records are;
- what the future of the functions to which the records relate to is;
- the decision for archival/destruction/transfer of record;
- responsibility and mechanism for transferring/destruction of records;
- what information is being shared and with whom.

Functions & Categories of Records

It may be helpful to consider the categorisation of functions and the associated records, in particular identifying those records that are likely to contain personal or confidential information. Although not all records will easily be grouped, the following categories might be helpful as starting point to facilitate thinking - these are reflected in the retention schedule at Annex D:

- Health Records
- Personnel/HR records
- Financial
- Estates
- Administrative
- Other

Inactive Records

Whilst active records should follow the associated function where this will continue, inactive records require additional consideration, particularly where they contain personal and/or confidential material. Inactive records that have no relevance to the new body should only be transferred where an organisation is closing, the records cannot yet be destroyed due to retention requirements and there are no suitable archiving arrangements.

Where records also contain sensitive information (e.g. inactive health records) that should not be shared with the new body without patient consent the situation is more complex. In these circumstances both the transferring and receiving bodies need to work closely to make

---

[3] When developing the information inventory equal consideration will need to be given to paper and electronic records. The National Archives have produced some useful guidance on Digital Continuity which can be found at http://www.nationalarchives.gov.uk/information-management/our-services/digital-continuity.htm

arrangements for secure archiving in a National Archives place of deposit (PoD) that will enable the tracing and re-activation of records[4], or the provision of a copy when needed, with the receiving body putting in place procedures for obtaining the necessary consents for retrieval.

Where it is not practicable to separate out inactive records from similar active records then the public interest will justify the transfer of all the records to the new body. Where this involves personal data appropriate steps need to be taken to prevent records being viewed by individuals who do not need to see them, e.g. access controls and/or logical deletion of the inactive records.

Personal Data & Information Governance

Throughout the transition, organisations must ensure that they adhere to Information Governance (IG) principles. Particular attention must be paid to the handling of identifiable and confidential information, such as that held in health or personnel records, as this information will require extra consideration when archiving, destroying or transferring.

All health records must be passed to an appropriate responsible body before an organisation is dissolved. No personal information, particularly health records, should be left without an appropriate data controller.

Where the information associated with a function includes confidential patient records it is essential that the transfer is tightly managed, the receiving organisation is working with the NHS Information Governance Toolkit and demonstrating a satisfactory level of performance and that there is a communications plan for informing the patients concerned about the change.

Where a change is internal to the NHS, the staff involved are largely the same and patients are unlikely to notice significant change, appropriate communications might be a short information notice being included in the next appointment letter or other communication. Where a change is more significant, e.g. an NHS service transferring to a private sector supplier, it may be necessary to write to each patient to explain the change and who to contact with any concerns and to do this in advance of any transfer.

The Department of Health's Information Security Management[5], Confidentiality[6] and Records Management [7]codes of practice also provide more detail about managing information confidentially and securely, and applying considerations to practical records management functions.

---

[4] s4(6) of the Public Records Act 1958, enables NHS bodies to request the temporary return of transferred records for operational purposes, for example in relation to a further episode of patient care.

[5] Department of Health Information Security Management: NHS Code of Practice - http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074142

[6] Department of Health Confidentiality: NHS Code of Practice - http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

[7] Department of Health Records Management: NHS Code of Practice - http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

Quality & Future Use of Information

Organisations must consider the quality and the usability of records which they are archiving or transferring. Information will only retain its value if it can be found, accessed, read and understood. Organisations should ensure that they use adequate filing systems when transferring information and consider compatibility and file types used for electronic media. If an organisation has decided to transfer all paper records to digital format (for example putting all finance records onto a DVD) to transfer to a new organisation, the records must then be checked to ensure everything has copied over correctly and can be viewed appropriately in the digital format before any paper records are then securely destroyed.

If creating a transferable archive of such documents, best practice would be to copy them in the formats that they are in, but in addition convert all documents to open, non-proprietary formats that will remain readable without requiring the same software they were created in. For example:

- Excel to csv format
- Word to pdf format
- PowerPoint to pdf format

Contracted out functions/records

It may be necessary to transfer a contract from one body to another. In some cases an in-house service may be transferring to a contracted supplier with the contract being held by a third party.

In any case it is important to be clear which legal entities a contract is between and to allow sufficient time for contract changes to be negotiated/agreed or for new contractual arrangements to be put in place.

In order to perform a function the contracted organisation will require access to the records that support that function. A 'Business Transfer Arrangement' may be useful to define schedules and clauses that cover the transfer, storage and handling of records during the contracted period and any 'handover/transition' periods

Support & Archiving

In cases where organisations are unsure what to do with records they should seek advice at an early stage from local National Archives places of deposit (PoD) [8] and from the Departmental Records Office (DRO) at the Department of Health.

The DRO is able to provide archiving facilities where organisations are being dissolved and have records which must legally be retained, however this facility should only be considered as a last resort and organisations must endeavour to make alternative arrangements. Agreements to transfer records to the DRO will be taken on a case-by-case basis and consideration will

[8] There is a general statutory duty "to make arrangements for the selection of those records which ought to be permanently preserved and for their safe-keeping". This is to be done under National Archives' supervision. Section 3(1) and (2) of the Public Records Act 1958.

need to be given to the medium that records are held on to determine whether the DRO has the facility to accept the records.

Annex A - Frequently Asked Questions

Q1. We are a PCT and we are transferring our GP out of hours service to the local NHS trust. Do we have to tell our patients and if so how - do we have to write to them all individually?

Patients need to be informed about changes to the way that services are provided and which organisations will be involved in their care and have access to their records. Where a change is internal to the NHS like this one and patients are unlikely to notice significant changes in the provision of services, appropriate communications might be leaflets and posters in GP surgeries and short information notices being included with GP appointment letters or other communications. It is not necessary to write to every patient in cases like this.

Q2. We are a PCT and our GP out of hours (OOH) service is going to the local NHS trust and our health visitor service to a new social enterprise. We currently have a shared record - can we make a copy of the record for each new provider or do we have to split the record?

The only safe solution is to provide a copy of the record to each of the new providers as both have a need to know. A communications plan for informing patients will be required but the efforts taken to inform will depend upon the specific circumstances. See the previous answer for communications relating to the transfer of OOH provision. Health visitors should be briefed on how best to reassure patients and should provide leaflets explaining the change to patients when they are doing their rounds. A point of contact for raising any concerns might also be provided.

Q3. We are a PCT and some of our provider functions are going to a social enterprise. Is there a difference between transferring records to an NHS organisation and a non-NHS organisation?

There is no legal difference but an important test that should always be applied is the extent to which patients would be surprised by a change. Some patients may be concerned about their records being held by a social enterprise and will need reassurance. This needs to be factored in to both the content of communications with patients and the means of communicating. Making patients aware of a change like this in circumstances where they can ask questions and receive reassurance may be the best answer, depending upon the nature of the service.

Q4. We are a PCT and we are negotiating a contract with the local Mental Health Trust to host some of our community services for a period of 3 years. I'm not sure that I understand data controller responsibilities and where they sit in these circumstances?

This depends upon the terms of the contract. If the Mental Health Trust is contracted to provide a service, perhaps with some specified deliverables, but is free to do this as it sees fit, and the PCT has no access to patient data or any authority to direct the Mental Health Trust in how it conducts the business, then the Mental Health Trusts is the sole

data controller. However, if the contract provides the PCT with the authority to direct the Mental Health Trust in respect of the way it processes patient data, then both may be data controllers in common. Prior to the PCT being abolished it will be necessary to formally transfer responsibility for delivery of the service to the Mental Health Trust or to formally transfer the contract to a continuing legal entity.

Q5. We are an SHA and some of our corporate functions (e.g. estates) are closing when we close. We have copies of records that are held on paper and electronically, do we have to archive both sets of records or can we just keep the electronic ones?

It is not necessary to archive duplicate records and electronic records are clearly cheaper to archive than paper. It is essential however that the electronic copies are checked to ensure they are complete and accessible and the means of accessing the information must be available and understood at the archive. The archive must also have policies and plans in place to support the transfer of data onto new media when systems changes would preclude access to older media. Best practice would be to copy them in the formats that they are in, but in addition convert all documents to open, non-proprietary formats that will remain readable without requiring the same software they were created in. For example:

- **Excel to csv format**
- **Word to pdf format**
- **PowerPoint to pdf format**

Q6. How do we make sure that we transfer our patient records and electronic patient records securely to the new providers of services?

Guidance on the secure transfer of records is available in the Information Governance toolkit https://nww.igt.connectingforhealth.nhs.uk/ - see requirement 308.

Further guidance can also be found at http://www.nationalarchives.gov.uk/information-management/guidance/a.htm

---

Q7.The organisation contracted to provide mental health counselling services goes into administration. What should be done to ensure the records are secure?

The contract ideally should have specified that all patient records should be transferred securely to either the contracting organisation or a secure archive – if the contract is not clear this should be negotiated. Standard retention policies should be followed to determine whether records can be destroyed or archived. Care should be taken to ensure that held records can be traced and transferred to a new provider if needed.

Q8.The provider service has been providing services for 15 years but is no longer the provider for community services, should all the information including those of inactive patients be transferred to the new provider?

Inactive health records should not normally be shared with a new provider without patient consent. The old provider should retain responsibility for the inactive records and follow the appropriate retention guidelines (hold, destroy or archive). A register of the inactive records should be created detailing the location of each to facilitate tracing if necessary. Where it is not practicable to separate out inactive records from similar active records then the public interest will justify the transfer of all the records to the new body, but appropriate steps need to be taken to prevent records being viewed by individuals who do not need to see them, e.g. access controls and/or logical deletion of the inactive records.

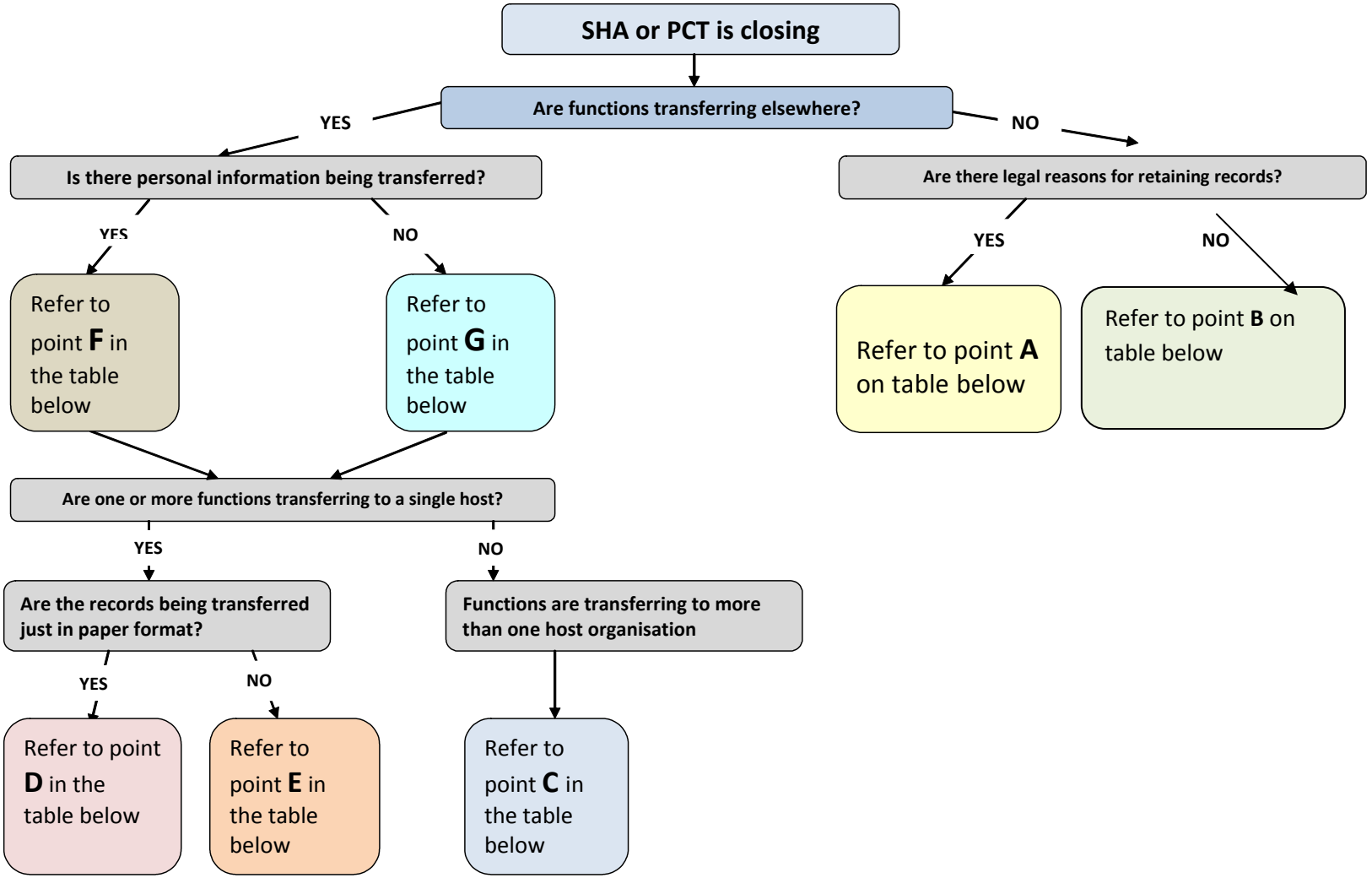
Q9. Where an NHS service is transferring to a private sector supplier, who takes responsibility for writing and explaining changes to the patient?

This may be subject to a local agreement but the responsibility to ensure it happens rests with the original service provider and the communications should take place prior to the transfer. If, for some reason, the original service provider fails to do this they are likely to be in breach of Data Protection legislation and other legal requirements. The new provider should seek confirmation that this communication has occurred before accepting the records. If the new provider accepts the records in circumstances where the communication has not taken place, as the new data controller it will need to take action to inform patients itself.

Q10. How should historical FOI and subject access requests be handled. Who do they belong to? Would it result in new information sharing arrangements being made?

The holder of a record is responsible for satisfying legal requests for information. Responsibility for complying with the law transfers with the record.

Annex B – Transfer of records flow chart



A	Some records may need to be retained for legal reasons for a minimum period of time following closure of the organisation; for example o Finance o HR o Estates If these records are not needed to support a business function but must be retained for legal reasons the transferring organisation will be responsible for ensuring that records are transferred to an appropriate Place of Deposit – more guidance on this can be obtained from The National Archives. Significant records (that are likely to require attention) have been highlighted in worksheets in Annex D**.**
B	Any records that have reached their minimum retention period and are no longer required to support a business function should be destroyed under confidential conditions – Records likely to fall into this area have been highlighted in Annex D.
C	Where personal information is involved only information that each host should see should be provided. This may involve photocopying sections of paper records so that each hosting organisation has the correct record.
D	**Paper records** – must be securely transferred to the new hosting organisation, with a high level list of the records being transferred to be signed by the new organisation (this will then provide some evidence of new ownership and responsibility for the records.
E	**Electronic records** – any electronic records relating to a function will also need to be transferred to the new hosting organisation, ensuring that these records can be accessed prior to final destruction (at the closing organisation). Access to records may be dependent on specific hardware/software and this will need to be considered (by an Information Transition Group) thoroughly during the transitional period. Annex C of this document will be particularly useful when considering these issues.
F	Where functions are transferring to a single host the organisation will require all original records relating to those functions and will then become the data controller for the records. Any records not being transferred (as they do not support a business function) will need to be destroyed under confidential conditions.
G	Where no personal information is involved it may be simplest to send complete copies of all records to each new host.

Annex C - IG Risk Checklist – Transfer of functions

	Information Risk Management – Joint Planning	Done?
1.	Conduct IG risk assessments at both transferring and receiving organisations taking into account changes arising from the transfer. For example, is there sufficient resource, secure storage etc at the receiving organisation?	
2.	Determine whether any personal information is to be transferred and if so, what quantity.	
3.	Confirm the receiving organisation meets all necessary IG security standards as identified within the IG Toolkit and has updated its security policies where necessary to accommodate the transfer.	
4.	Record the outcome of the IG assessments and the risk management decisions in each organisation's IG risk register.	
5.	Ensure all organisations have a good understanding of the IG risks involved in the transfer.	
6.	Ensure there is full Information Asset Owner oversight and involvement for each information asset during the period of transition.	
7.	If information assets and business processes are to be split amongst several organisations, determine the practical working arrangements during the transfer and ensure appropriate IG risk management responsibilities following the transfer.	
8.	Decide how the secure transfer of information assets will take place, following the guidelines on secure transfer in the IG Toolkit. User rights to transfer information to removable media should be strictly limited and be in accordance with agreed business need.	
9.	Decide whether there will be any additional compromise or threats to information assets during transfer and whether any additional personal, electronic or physical security measures will be required to protect information systems.	
10.	Take account of any changes to external connections to N3 and other systems (closing old or establishing new connections). Consider the IG implications this may have for other organisations potentially affected.	
	Business Continuity – Joint Action	
11.	Ensure appropriate Business Continuity and Disaster Recovery Plans are in place and are updated as functions are transferred.	
12.	Determine whether any other organisation(s) could provide a contingency service if a disaster occurs.	

13.	Determine whether less critical services may be temporarily discontinued until the transfer or merger is completed.	
14.	Decide whether any parallel running might be needed during transfer with the same information used on two systems.	
15.	Consider all business dependencies and impact of compromise or interruption to those services, e.g. should records be inadvertently lost, damaged or destroyed during transfer. This should include the effect on all organisations having an interest in the records, not just the current data controller (for example voluntary and charitable organisations working with NHS trusts).	
	Transferring Organisation	
16.	Revise access controls and system privileges of staff, contractors and others at the transferring organisation in a timely manner.	
17.	Consider a formal knowledge capture exercise to document knowledge of staff who are leaving the organisation.	
18.	Ensure all media used for storing or processing confidential or protectively marked information is disposed of or sanitised in accordance with NHS IG guidelines. Equipment may be particularly vulnerable when staff leave and equipment is left in situ or in unattended storage – but not yet decommissioned.	
19.	Ensure vital information is backed-up and physical storage issues are resolved.	
	Receiving Organisation	
20.	Ensure an up-to-date IG toolkit assessment has been completed.	
21.	Identify staff training requirements as soon as possible and plan delivery.	
22.	Ensure that all key information about any transferred records is obtained (metadata).	
23.	Ensure required systems are in place and access rights are appropriately assigned.	
24.	Ensure all transferred records have owners and that all relevant records & information management policies have been updated accordingly.	
25.	Ensure all transferred records have appropriate retention and disposal schedules in place.	
	Shared Services	
26.	Determine whether any services are currently shared and whether they need to be transferred.	
27.	Review any formal contracts and Service Level Agreements and their penalties if the contract/SLA is terminated early, or services are not	

	delivered.	
28.	If the shared service is to be transferred, decide how existing services will be maintained, or agree a reduced service for the transitional period.	
29.	Consider the immediate business impact and costs of terminating ongoing projects or programmes, especially security-related ones.	
30.	Check all relationships (including with customers and stakeholders) and how they may be affected by the transfer of services.	
31.	Assess the likely impact (on customers, reputation etc) if shared services are interrupted during or following the transfer.	
32.	Produce a communications plan to ensure customers, stakeholders, staff etc are effectively informed of the change in service delivery.	
33.	Produce a problems management plan.	
34.	Maintain a website holding page where appropriate to inform those not reached by general communications.	

Annex D - Records retention schedules

An Excel Spreadsheet containing 4 separate worksheets accompanies this guidance.

These retention schedules have been adapted from the Department of Health's Records Management NHS Code of Practice. They are specifically prepared for use during the current (2011/12) transition. Schedules from the main Code of Practice should be used for future records management outside of transition as they are updated at intervals.

Annex E – Further Guidance

The National Archives

General Guidance on Organisational Change:

www.nationalarchives.gov.uk/information-management/projects-and-work/reform-public-bodies.htm

Managing and Maintaining the Usability of Digital Information Through Change:

www.nationalarchives.gov.uk/information-management/our-services/digital-continuity.htm

General Guidance on Records and Information Management:

www.nationalarchives.gov.uk/information-management/projects-and-work/information-records-management.htm