Yorkshire and the Humber Strategic Health Authority **BOARD MEETING**	NHS Yorkshire and the Humber
Date: 6 July 2010	**Report Author:** Joanne Dally
Title of paper: Information Governance Policies: Information Governance Policy & Strategy (v3); Data Protection and Confidentiality Compliance in Changes to Business Processes, New or Upgraded Information Systems	
Actions Requested: The Board is asked to approve revisions to the Information Governance Policy and Strategy following annual review and to approve a new procedure for Data Protection and Confidentiality Compliance in Changes to Business Processes, New or Upgraded Information Systems	
Governance Requirements	
SHA Objectives supported by this paper: Making Yorkshire and the Humber SHA an excellent organisation	
Risk Management: Relates to risk 3.2 (2010/11 Board Assurance Framework): SHA internal systems and processes fail to support the effective governance, operation and resilience of the organisation, including in relation to the discharge of its statutory functions	
Board Assurances: Implementation of this procedure will provide additional assurance on the SHA's compliance with Data Protection and confidentiality requirements	
Risk Assessment: The main risk identified with this procedure is non-compliance. The Health Informatics Service (THIS) are the originators on the procedure and would also be involved in changes to business systems and so will be able to ensure that the process is completed.	
Communication (including public and patient involvement): Once approved the procedure will be communicated to all staff via the Weekly Update	
Resource Implications – including productivity and value for money: No additional resource needs identified	
Legal Implications No specific legal advice required	
Equality and Diversity No E&D issues have been identified in relation to this report	
NHS Constitution: This report is compliant with the NHS Constitution	

Yorkshire and the Humber Strategic Health Authority

6 July 2010

Information Governance Policies

i) Information Governance Policy and Strategy

The SHA is required to review its Information Governance Strategy annually. The only significant change following the latest review is to merge the former Information Governance Group with the Information Management and Technology (IM&T) Strategy Group.

Revised terms of reference for the group are appended to the Strategy.

Information Governance activities take place in several areas of the SHA and is overseen by the IM&T Strategy Group. The Group reports via the Business Assurance Group to SMT and the Audit Committee.

ii) Data Protection and Confidentiality Compliance in Changes to Business Processes, New or Upgraded Information Systems

A new procedure has been developed by the Health Informatics Service to ensure that compliance with Data Protection and Confidentiality obligations are discharged in the event of changes to business systems and processes.

Recommendation

The Board is asked to approve these policies.

Prof. Sue Proctor
Director of Patient Care and Partnerships (Senior Information Risk Owner)
6 July 2010

NHS
Yorkshire and the Humber

Information Governance Policy and Strategy

Version 3

Policy Reference Information

Policy Name	Information Governance Strategy & Policy
Version	3.0
Status	Draft
Originator/Author	Joanne Dally
Responsible Director	SIRO
Approved By	SHA Board
Date Issued	
Last Review Date	July 2010
Next Review Date	July 2011
Applies to	All SHA staff (including hosted programmes)

Document Revision Record

Version	Description of Changes	Reason for Change	Author	Date
3.0	Revisions to terms of ref.	Amalgamation of IG and IM&T Strategy groups	B Gill	May 2010

Related Information, Policies and Legislation

SHA Confidentiality Policy Statement & Guidance	Data Protection Act 1998
The NHS Confidentiality Code of Conduct	Freedom of Information Act 2000
SHA policy and Procedure for Responding to Requests under the Freedom of Information Act, 2000	Human Rights Act 1998
SHA Policy for the Production, Retention, Publication and Destruction of Records (incorporating the Retention Schedule)	Environmental Information Regulations 2005
SHA Procedure for Archiving Paper Files	Access to Health Records Act, 1990 (where not superceded by the Data Protection Act
SHA Incident Reporting Policy	Common Law Duty of Confidentiality
SHA E-mail policy	The Caldicott Report, 1997
SHA Internet policy	
SHA Business Continuity Procedures	

Contents

Yorkshire and the Humber Strategic Health Authority

Information Governance Policy and Strategy

1. Introduction

The SHA recognises the importance of reliable information to enable its efficient functioning and operation and compliance with relevant legislation. Information governance plays a key part in supporting the effective conduct of SHA business. It is also core to enabling the SHA to fulfil its obligations under legislation including the Data Protection Act and Freedom of Information Act.

Effective information governance processes give assurance to the SHA and to individuals (including patients, the wider public and staff) that confidential information, including personally-identifiable information, is dealt with securely, efficiently and effectively and in compliance with legislation.

The SHA has established and maintains policies and procedures in compliance with requirements set out in the Information Governance Toolkit developed for the NHS by Connecting for Health as a benchmark for best practice in information governance.

2. Scope

This policy covers all aspects of information within the SHA and its hosted programmes, including (but not limited to):

- Patient/Client/Service User information
- Staff/Personnel information
- Organisational information

This policy covers all aspects of handling information, including (but not limited to):

- Structured record systems - paper and electronic
- Transmission of information – fax, e-mail, post and telephone

This policy covers all information systems purchased, developed and managed by/or on behalf of, the SHA and any individual directly employed or otherwise by the SHA.

3. Principles

3.1 Openness

- The SHA recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

- Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the Data Protection Act (DPA). Information held by the SHA that is not subject to the DPA is subject to requirements set out in the Freedom of Information Act 2000. The SHA's Policy and Procedure for Responding to Requests under the Freedom of Information Act sets out the SHA's obligations under the Act.
- Individuals have rights of access to information relating to them in accordance with the Data Protection Act. Arrangements are in place to respond to queries from patients and the public that fall within the scope of the Data Protection Act. Requests under the DPA are handled by the SHA's FOI lead (Associate Director – Corporate Business).
- The SHA has clear procedures and arrangements for liaison with the press and broadcasting media.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- Availability of information for operational purposes will be maintained and retained in accordance with the SHA's records management policies and retention schedule and protected via appropriate computer system resilience and business continuity procedures.
- All identifiable personal information will be treated as confidential and managed in compliance with legal and regulatory frameworks. Breaches of confidentiality must be reported in accordance with the SHA's Incident Reporting policy.
- The SHA has established and maintains policies and procedures to ensure compliance with relevant legislation, including the Data Protection Act and the Freedom of Information Act.
- Information Governance training is provided to all staff to support awareness and understanding.
- Risk assessment is undertaken to ensure effective and appropriate information governance controls are in place.

3.2 Information Security

- The SHA has established and maintains policies for the effective and secure management of its information assets and resources.
- Audits are undertaken to assess information and IT security arrangements.
- An Incident Reporting system is used to report, monitor and investigate all breaches of confidentiality and security.

3.3 Information Quality Assurance

- The SHA has developed policies for the management of records and is working to develop information quality assurance.
- Managers are expected to take ownership of, and seek to improve, the quality of information and information governance and management within their business areas.

4 Related Policies

The SHA has developed a range of policies supporting the information governance agenda; reference must be made to these alongside this policy. Specialist Information Governance, Information Security and Records Management advice is available to the SHA. Legal and additional professional guidance is also considered where appropriate.

5. Assessment and Improvement

An assessment of compliance with the requirements of the Information Governance Toolkit (IGT) is undertaken annually and signed off by the SHA Board. Reports and proposed action/development plans are agreed by the Information Management and Technology (IM&T) Strategy Group, which reports via the Business Assurance Group to the Audit Committee.

6. Training

The training needs of SHA staff will be assessed as part of the SHA's training and development planning. Information Governance has been designated by SMT as an element in a package of essential training to be provided to all staff. The Service Level Agreement with the Health Informatics Service includes the provision of IG training for all SHA staff.

7. Information Governance Management

Information governance management across the organisation is co-ordinated by the IM&T Strategy Group. Terms of reference, membership and other details about the operation of the Group are appended.

Appendix

Yorkshire & The Humber SHA
Information Management and Technology (IM&T) Strategy Group

Terms Of Reference

PURPOSE

The Yorkshire & The Humber IM&T Strategy Group provides a forum for the SHA and its hosted organisations for leading on the development and implementation of an IM&T Strategy and the management of the IM&T Service. This is mainly through services provided by The Health Informatics Service, including information governance. which support the business of the SHA. The Group will initially focus on developing the required structures, policies and procedures, and then maintaining these. Subsequently the Group will manage the delivery of the IM&T Service. It will also provide the forum for overseeing the work of THIS contract, including information governance (IG), and for ensuring IG work needed is underway.

SCOPE

The scope of the group will include the following:-

- Yorkshire & The Humber SHA IM&T Strategy
- Yorkshire & The Humber SHA IM&T Systems and Services including telephony
- Systems and services provided by Yorkshire & The Humber SHA to third parties including hosted organisations
- Systems and services provided to Yorkshire & The Humber SHA by third parties including THIS
- The SLA between Yorkshire & The Humber SHA and THIS
- Information governance for the SHA
- The development and implementation of SharePoint and other IT programmes for the SHA

DELIVERABLES

The deliverables of the group will include the following:-

- Ensuring that the business objectives of the SHA are represented and met by the IM&T Strategy
- Agreeing, publishing and implementing organisational structures including any sub-groups
- Agreeing, publishing and implementing individual responsibilities
- Developing and publishing an IM&T Strategy and linking this as appropriate to the NPfIT programme and associated Digital

Strategy to support the delivery of the national programme and High Impact Change areas identified by the national CIO Forum.

- Ensuring that System Availability meets the business requirements of the SHA and underpins Business Continuity
- Managing the SLA with The Health Informatics Service
- Managing the escalation and prioritisation of IM&T issues
- Initiating internal SHA IM&T Projects
- Evaluating and recommending technology solutions to support the business needs and business plan
- Developing, maintaining and publishing policies and procedures associated with IM&T issues
- Reporting on the performance of the IM&T SLA
- Developing working relationships with key internal and external stakeholders
- Acting as the primary contact point for consultation on any matters relating to IM&T
- Providing an open forum opportunity for others to interact with the SHA on IM&T issues
- Providing the communication link to the rest of the organization on IM&T issues, including via directorate representatives, who have responsibility for ensuring their teams are made aware of these.

GOVERNANCE

- This group is sponsored and directed by the Board of the SHA
- This group is accountable to the Senior Information Risk Officer (SIRO) of the SHA
- Decisions taken by this group will be endorsed by the SIRO
- Recommendations made by this group which affect the business of the SHA will be considered and actioned by the Senior Management Team (SMT), as needed
- The Terms of Reference for this group will be developed and maintained by the membership of the group.
- Formal approval of the Terms of Reference will be given by the Board of the SHA
- Meetings will have an agenda
- Meetings will be formally minuted
- Minutes will be provided to the Business Assurance Group
- The IM&T Strategy Group will adhere to the values and functions of the SHA, and in particular recognise its role under thought leadership, capacity building and advocacy and interpretation.

LINKS

This group will necessarily require links with other groups, particularly:-

- Yorkshire and the Humber SHA Board
- Senior Management Team (SMT)
- Sub-groups of the IM&T Strategy Group

- The NPfIT programme groups
- The collaborative High Impact Changes (Informatics) programme groups
- Business Assurance Group
- Audit Committee
- Don Valley House User Group
- Business Managers Group
- ESR/SBS
- Health Service Observatory
- Cancer Screening Service
- Staff Partnership Forum
- THIS (principally via the account manager, and IG lead)
- The SharePoint programme team
- Quality Observatory

MEMBERSHIP

Chair:– Bridget Gill

Members:- Trevor Wright (technical lead)
Chris Dunne (THIS Account Manager for NHS YH)
Trevor Parsons (IG lead)
Helen McNae (THIS IG lead for NHS YH)
Jo Dally (corporate lead including policy lead)
Forrest Frankovitch (or representative)
Facilities Managers – Jan Rye and Richard Thomas
Kath Little (business manager to provide admin support)
Representatives from directorates

Suitable deputies can attend with prior notification.

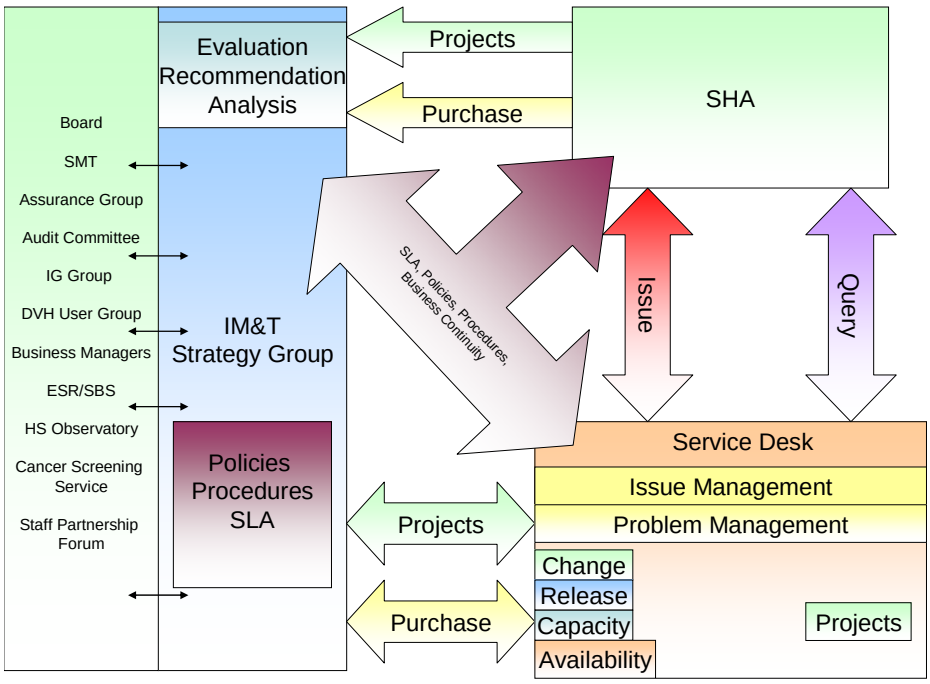
MEETINGS

Monthly and face-to-face where possible (or by telecom or with telecom link as needed)

Where appropriate the group will discuss and decide on working practice. Where a strategic decision is needed then the group will make recommendations to SMT and other forums, as needed, ensuring that the SIRO is kept informed as appropriate.

REVIEW

These Terms of Reference will be kept under review to ensure appropriateness in a dynamic environment.


Evaluation
Recommendation
Analysis
Projects
Purchase
SHA
Board
SMT
Assurance Group
Audit Committee
IG Group
DVH User Group
Business Managers
ESR/SBS
HS Observatory
Cancer Screening Service
Staff Partnership Forum
IM&T
Strategy Group
SLA, Policies, Procedures, Business Continuity
Issue
Query
Policies
Procedures
SLA
Service Desk
Issue Management
Problem Management
Projects
Purchase
Change
Release
Capacity
Availability
Projects

NHS
Yorkshire and the Humber

Data Protection and Confidentiality Compliance in Changes to Business Processes, New or Upgraded Information Systems

Data Protection Act 1998 and Associated Legislation

Policy Name:	Data Protection and Confidentiality Compliance in Changes to Business Processes, New or Upgraded Information Systems
Version	1.0
Status:	Draft
Name of originator/author:	Confidentiality and IM&T Security Officer (THIS)
Responsible Director:	SIRO
Recommended by:	IM&T Strategy Group
Approved by:	SHA Board
Issue date:	
Review date:	July 2011
Applies to:	All Staff

Data Protection and Confidentiality Compliance in Changes to Business Processes, New or Upgraded Information Systems

1 Introduction

The introduction of new internal business processes (facilitated by information systems) and new or upgraded information systems could potentially result in the SHA breaching the principles of the Data Protection Act 1998 and other associated legislation.

It is essential that any systems (or new business processes) which hold and use person identifiable information (patient or staff information) are tested for data protection and confidentiality compliance before they are procured or implemented. Where necessary, small scale or full scale Privacy Impact Assessments may then be recommended (in line with the Information Commissioner's Privacy Impact Assessment Handbook).

Data Protection and Confidentiality assessment is most effective when started at an early stage of a project, when:

- The project is being designed
- You know what you want to do
- You know how you want to do it, and
- You know who else is involved.

Ideally it should be started before:

- Decisions are set in stone
- You have procured systems
- You have signed contracts/Memorandum of Understanding's/agreements, and
- While you can still change your mind!

It is vitally important that all proposed changes to the SHA's IT systems and processes are able to maintain the confidentiality, integrity and accessibility of information.

This document details the actions to be taken before departments, areas or functions implement changes to internal business processes or procure new/upgraded information systems.

The attached compliance questionnaire will assist you in considering whether a new/upgraded information system or process will:

- Allow personal information to be checked for relevancy, accuracy and validity
- Enable the integrity of personal information to be maintained
- Incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required
- Have adequate levels of security to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction or damage

- Enable the timely location and retrieval of personal information to meet subject access requests
- Transfer personal data outside the European Economic Area (EEA)

2 Steps to ensuring Compliance

There are five steps to ensuring that data protection and confidentiality issues have been properly considered and managed prior to procurement and implementation of changes to internal business processes and information systems. The five steps are detailed below and also set out in the flow chart at Appendix A:

Step 1 – Project Initiation
Managers and/or members of staff leading changes to business processes and the procurement of new or upgraded information systems must initially complete the questionnaire: Data Protection and Confidentiality Compliance Questionnaire (Appendix B), to initiate an assessment of data protection and confidentiality compliance.

The need for consultation must be communicated to all staff members who are involved in the procurement of any changes to systems and in the process design.

The completed questionnaire should be submitted to the Confidentiality and IM&T Security Service, THIS.

Step 2 – Review of Completed Questionnaire
The Confidentiality and IM&T Security Service, THIS will consult with you in respect to answers given on the questionnaire and help to identify any areas of risk.

Step 3 – Risk Assessment
Any identified risks should be formally assessed and a risk treatment plan put in place to reduce the risk. Risks should be logged on the relevant departmental risk register. It is the responsibility of the Project/Change Initiation lead to ensure risks are assessed, treatment plans put in place and entries made on the relevant risk register.

Step 4 – Agreement to Proceed
Sign off via the SHA's Senior Information Risk Owner/Caldicott Guardian to show that the SHA is satisfied that all data protection and confidentiality issues have been resolved or that proposed actions that would be needed to be put in place to reduce an identified risk, have been outlined via the SHA risk assessment process.

Where a Business Case/Project Initiation Document is to be put together at the outset of the project, ensure this includes details of all risks identified and detail of steps taken to mitigate risks.

Step 5 – Post Implementation Risk Assessment
The Project /Change Initiation lead for the new business process or information system should ensure that following implementation, a post implementation data protection and confidentiality risk assessment is

undertaken to ensure that there are no new risks. It is expected this would be conducted as part of the overall evaluation of the project.

All completed questionnaires will be filed as evidence that data protection and confidentiality compliance checks have been undertaken in accordance with requirement 210 of the Information Governance Toolkit.

3 Flow Chart Procedure

See Appendix A for flow chart procedure.

4 Support and Advice

For further explanation of the questionnaire and process, please contact: Confidentiality and IM&T Security Service, THIS.

5 Sample Questionnaire

See Appendix B for sample completed questionnaire.

6 Related Policies

Confidentiality Policy and supporting guidance.

7 Glossary of Terms

Subject Access Request - A request by a data subject (patient, member of staff) to view personal data from an organisation

Automated Decision Making - The use of computers to carry out tasks requiring the generation or selection of options.

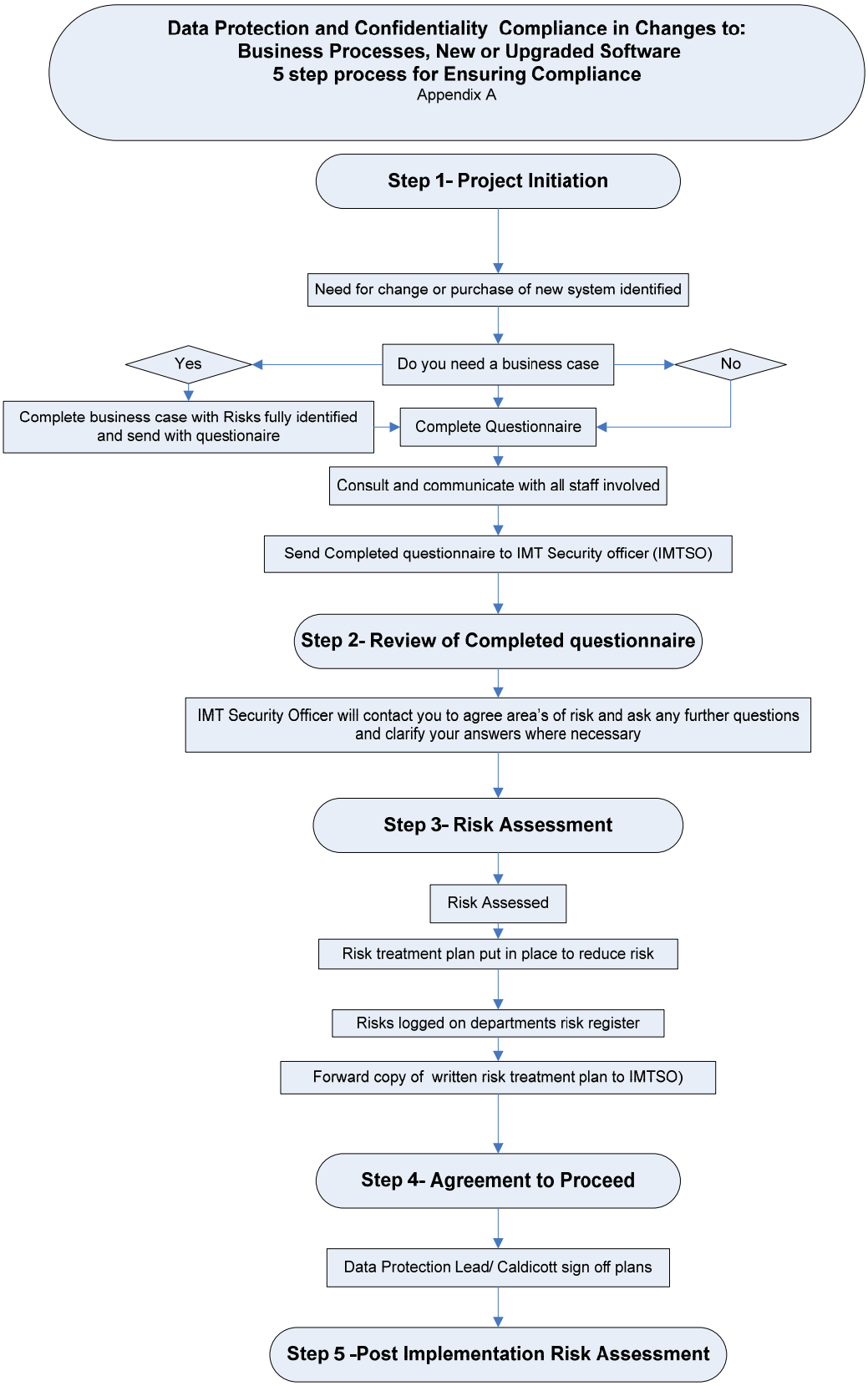
Third Party Data Processor - Contractor working for a Data Processor who processes personal information on behalf of the SHA (data controller).

Full scale PIA - An in depth internal assessment of privacy risks and liabilities, where there is wide consultation with stakeholders on privacy concerns.

Small scale PIA - Similar to a full scale PIA, but less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project.

8 Acknowledgements

North Bristol NHS Trust



LP
2007

Appendix A

Appendix B

Data Protection and Confidentiality Compliance Questionnaire

Please complete the questionnaire below. *(Completed to give example)*

For assistance in completing the questionnaire please contact the Confidentiality and IM&T Security Service on 0845 1272600.

Your name ***Please print***	
Job Title	
Contact Tel. Nos	Date

Implementation of MS SharePoint 2010 – eQUIP Programme

A Corporate Knowledge Management System which will support the needs of our organisation to increase the adoption of matrix working. The main aims of the eQUIP programme are : to ensure efficiency of all work carried out in a secure and stable environment with full compliance of our corporate policies and procedures, to enable collaborative working and reduce the carbon footprint for the SHA.

SharePoint 2010 will replace the current Intranet/Extranet to benefit the organisation with:

- A solution for records management
- Enhance collaborative working
- Increase knowledge and content management

SharePoint 2010 will also replace many paper based processes with smart electronic tools/applications such as the FOI request management, HR, Risk Management, Briefings, and Meetings etc.

Authorisation to Proceed (*official use only*)

Name of Authorised Lead	
Signature of Authorised Lead	
Date	

Answers to questions should be given by circling the appropriate answer i.e. YES, NO, N/A and/or by giving a descriptive answer in the answer box provided.

Purpose, Identification, Relevance and Accuracy

1. Does the system hold data that identifies individuals? **YES**
If 'yes' please identify if these are patients, staff or others and justify why the data has to be obtained and stored in an identifiable format.

The system will hold all the current files stored on our shared drives. It will store staff personal details, including the staff directory. This data is held for HR purposes, and to enable collaborative working. Any Person Identifiable Data will be open only to those with specified permissions.

2. What purpose does the collection of data serve?

Give an overview of the sort of information you will be recording

Name, Business Address, Contact Telephone Numbers (business landline and mobile), job title, areas of special interest. Photos (still to be confirmed).

3. Who will have access to the system?

This list need not be exhaustive, but identify the types of staff and roles

All staff working within the NHS in Yorkshire and the Humber will have access to the system, including NHS organisations on the N3 network. Access to information will be managed through security/permissions

4. Are the subjects (patients/clients/staff) of the data informed about the processing? **YES**

If yes, then how are they informed?

Yes. We currently hold this information. SPF (Staff Partnership Forum) to be informed.

5. How will accuracy of the data be maintained?

Through version control/retention rules along with Communications team policing the Intranet/Extranet content

Access Controls

6. How is the user identified to the system?

By unique username or shared access?

Both, unique username and shared access, however this depends on the level of access the user has been provided with and whether the user has access to the SHA network or just accessing the system from the N3 network. If user on the SHA network, they will have access to the Intranet with their unique username, if another NHS organisation, i.e. PCT, Trusts then Extranet view only with anonymous access.

7. How is the user verified by the system?

By password or other means?

By computer login password

8. Once logged in please describe any levels of access/function that are used that will allow different users to access different information and/or functions.

Users will be split in various groups, read/write/contribute/full rights can be allocated to users depending on the access level required.

9. Will the system access controls and access rights be described within a documented procedure for staff? **YES NO N/A**

Please explain your answer

Those staff that will have full rights will be trained as champions/super users. The rest of the organisation will be made aware through communications who to approach if they require any assistance as they may not have the access rights. Tight control on users' rights will be maintained by the System Administrator/IT.

Disclosure

10. Who will generally receive output (information) from the system (in addition to the actual system users)?

In effect all NHS employees are users, and those on N3 will also see the system. As the system is an intranet there is no output as such.

11. Will the information be transferred (or processed) outside the European Economic Area (EEA)? **YES NO N/A**

If Yes, to which country or territory?

No

Audits and Reporting

12. Will the system collect audit data on the activity of users (e.g. failed login report)? **YES NO N/A**

If Yes, please give basic details of what is to be recorded.

No

13. Does the system enable retrieval of information with regards to the rights of data subjects when making a Subject Access Request? **YES NO N/A**

Please explain your answer

Yes, for those people who have permissions to get at PID.

14. Does the system facilitate automated decision making? **YES NO N/A**

If Yes, please elaborate

No

Staff Training

15. Will staff training in the new business process or system include specific training/guidance in data protection, confidentiality, data quality and good practice in the management of records? **YES NO N/A**

Describe the proposed training provision

Yes, this will be outlined in the training material – currently being compiled by THIS.

Security of Information

16. Will there be a requirement for personal data to be moved/transmitted?
YES

If Yes, please describe how it will be transported/transmitted securely?

Staff Directory

17. Will any third party data processors be used by the supplier?
YES NO N/A

If Yes, please state name of third party and their role

No

18. Will there be a secure process for disposal/destruction of the data?
YES

Please explain your answer

Yes – this will be managed by retention rules – dates set on files for disposal/destruction, SHA has a full policy.

19. Where relevant, do the design and management arrangements for electronic systems incorporate appropriate controls against malicious code and unauthorised mobile code (computer viruses)?

Please explain

1) All seven servers have Sophos installed and are visible on the Sophos central management console. 2) All seven servers are newly-built and would have been fully patched at the time of building 3) The backup solution we have in place, i.e. all data (in the form of databases) is copied to NetApp central storage.

20. Where the SHA is working with a contractor to procure a new business process or software, does the contract documentation include clauses relating to information governance (data protection, confidentiality, freedom of information)?

NOTE The PASA Terms and Conditions of supply of goods and services should be used

Yes

This questionnaire should be returned to:

Confidentiality and IM&T Security Service
The Health Informatics Service
Oak House
Woodvale Road
BRIGHOUSE
West Yorkshire