

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:	Final - approved
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:	19 July 2010
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).

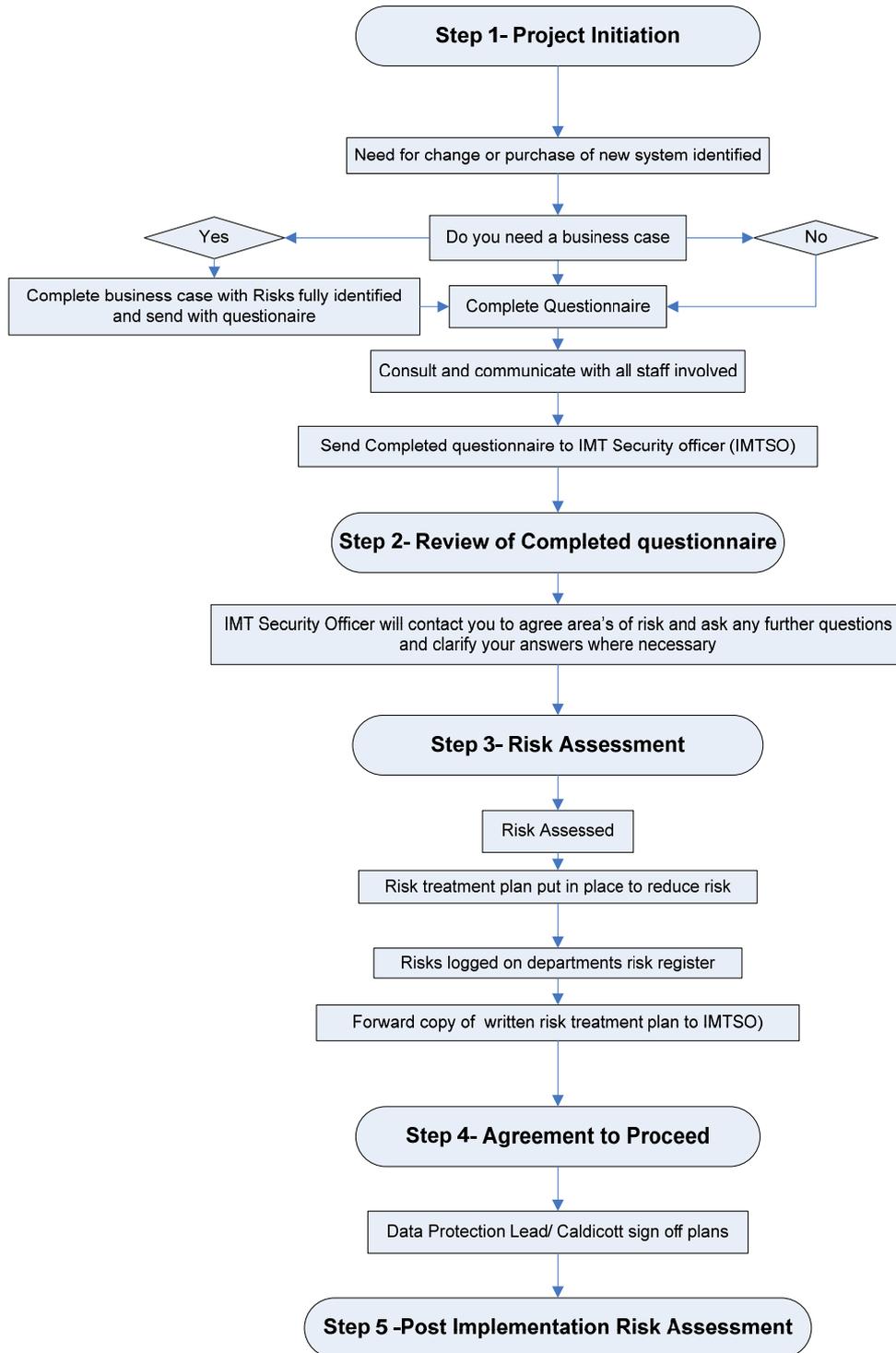
Full scale PIA - An in depth internal assessment of privacy risks and liabilities, where there is wide consultation with stakeholders on privacy concerns.

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

**Data Protection and Confidentiality Compliance in Changes to:
Business Processes, New or Upgraded Software
5 step process for Ensuring Compliance**
Appendix A



LP
2007

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**