Sample Privacy Impact Assessment Report Project: Outsourcing clinical audit to an external company in St. Anywhere's hospital

October 2010

Please Note: The purpose of this document is to demonstrate how the PIA process works and the format of a PIA Report. St. Anywhere's hospital is fictitious and is not intended to represent any hospital and no such project has been proposed. Certain assumptions have been made around policies and processes for the purpose of compiling this report.

Executive Summary

Background and introduction

St. Anywhere's hospital provides acute general hospital services to North Dublin. The hospital has 360 beds and treats 17,600 in-patients per annum. There are approximately 35,000 outpatient attendances annually and 31,000 patients attend the Emergency Department per annum. St. Anywhere's routinely conducts clinical audits for the purpose of improving the quality and outcome of patient care. The management of the hospital has proposed to outsource the function of clinical audit in order to benefit from external expertise and an unbiased examination of the quality of care provided to service users. This will also shift the focus of hospital resources and expertise to implementing recommendations from audits rather than on actually undertaking them.

Project description

The project will involve a tendering process, in line with procurement guidelines, following which the successful candidate will be contracted to the hospital on an as-needed basis to conduct on-site clinical audits. Clinical audit will, in the future, be conducted by an external auditor. However, all other aspects of the process will remain the same, as described in section 1 of this report. The project will involve a change to the current process in that the external auditor will need to access patient healthcare records and as such will have access to sensitive personal health information. As this change to the clinical audit process involves personal health information it is necessary to undertake a PIA to determine if it poses any privacy risks and if so to identify ways to mitigate these risks in the best interests of the hospital's service users.

The PIA process

The PIA was undertaken by the project lead with the assistance of the project team and additional members of the hospital staff. As a first step the project team completed a PIA threshold assessment, the outcome of which determined that it was necessary to proceed with the PIA process. In exploring the aspects covered in Stage 2, five privacy risks were identified, one of which remains an outstanding issue.

The privacy risks identified are as follows:

- medical professionals are bound by codes of conduct and owe a duty of confidentiality to service users. Each member of hospital staff has contractual obligations in relation to privacy. The external auditor may not be bound by these same codes of professional conduct, this may increase the risk of inappropriate disclosure of information
- due to change in practice the service users are not aware of proposed change in information practices and as such are not fully aware of how their information will be used. Service users have a right to know how their information is being used. Although implied consent is considered sufficient for clinical audit, service users need to be aware of this change in the clinical audit process and assured that appropriate safeguards to protect their privacy are in place
- the auditor may access additional patient healthcare records thereby accessing more personal health information than is necessary to complete the audit/unauthorised access to sensitive personal information. The risk in this instance is in relation to breach of access rights
- the auditor may use the information inappropriately, use it for secondary purposes or disclose it to another individual. Such misuse of information poses a risk to the privacy and confidentiality of service users and could result in the hospital being in breach of data protection legislation
- the auditor may know the service user whose record they are reviewing as part of the clinical audit process. Although this is a risk with the clinical audit process as it stands currently the service user could potentially be more uncomfortable with this proposal as the external auditor does not owe the same duty of confidentiality to the service user as a health professional.

Each of the five privacy risks were assessed in Stage 3 of the process with actions identified to mitigate four of these. This involved a consultation process with members of the hospital staff and service users to obtain their views and opinions.

The final stage of the process is the compilation and publication of this document – the PIA report.

Recommendations

Having completed the PIA the project team recommend that a number of actions be taken to uphold the privacy rights of service users. These actions combined serve to mitigate the risks identified in the course of the PIA. The actions required are:

that the tendering process is thorough and robust and the successful candidate can demonstrate its ability in this area and can demonstrate its ability and competence in dealing with sensitive and confidential information

- A legally binding contract of confidentiality is put in place between the hospital and the external auditor that details in full the obligations of the auditor in terms of confidentiality and protecting the privacy of service users. This will place the same duty of confidentiality on the external auditor as those conferred on health professionals by professional codes of practice

- That the hospital's statement of information practices is updated to include this change to the clinical audit process, thus keeping service users informed of the way in which the hospital uses their information

- Clear terms of reference are set for each clinical audit, indicating the information that will be necessary to complete it, with particular emphasis on the need to access patient healthcare records. These terms of reference will be adhered to by the hospital and the external auditor at all times

- The audit takes place in the healthcare records library and a process is developed whereby the auditor only has access to the records necessary to complete the audit. An audit trail will be kept to track records signed out and returned. When the records are not in use they will be held securely. The records will not leave the healthcare records library at any point.

- The external auditor will not have access to the hospital's Patient Administration System (PAS). Typically this may need to be accessed in the course of a clinical audit, for example to view results not yet in the medical record. The external auditor will instead be assigned a contact person who is a member of the medical records staff, who will access the necessary records on the PAS system as appropriate.

Table of Contents

1. Introduction and description of the project

The project involves outsourcing the clinical audit function to an external auditor. The hospital routinely conducts clinical audits with the specific aim of improving the quality and outcome of patient care. The ethos of the hospital is one that promotes and fosters continuous improvement and development and the benefits of clinical audit are very much understood and supported. The hospital is now proposing to outsource this function in order to benefit from external expertise and also to focus the resources of the hospital on implementing recommendations from audits rather than on actually undertaking them.

At present clinical audit is conducted on-site by clinical staff. At the outset of any clinical audit terms of reference are agreed. The auditor sources relevant information from patient healthcare records, stored in the healthcare records library in the hospital. An audit trail of records accessed and returned is kept by a member of the administrative staff and recorded in the clinical audit file. The information necessary for each specific clinical audit is extracted from the patient healthcare record and entered on a database specifically designed for each clinical audit. The service user's MRN (medical record number) is used as an identifier to input the data to the computer for analysis. Once the relevant information has been extracted the healthcare record is returned to a member of the healthcare records staff. All of this work is done on a computer in the healthcare records library (the records do not leave the library at any point). In line with the hospital security policy, auditors are not permitted to use a laptop or any portable storage devices for this work. The computers in the healthcare records library are password protected and information is stored on the hospital server, which is secure and is backed-up at regular intervals. Analysis of the data also takes place in the healthcare records library, with patients being identified at this point only by their medical record number (MRN). This process will remain the same except that the audit will now be undertaken by external auditors.

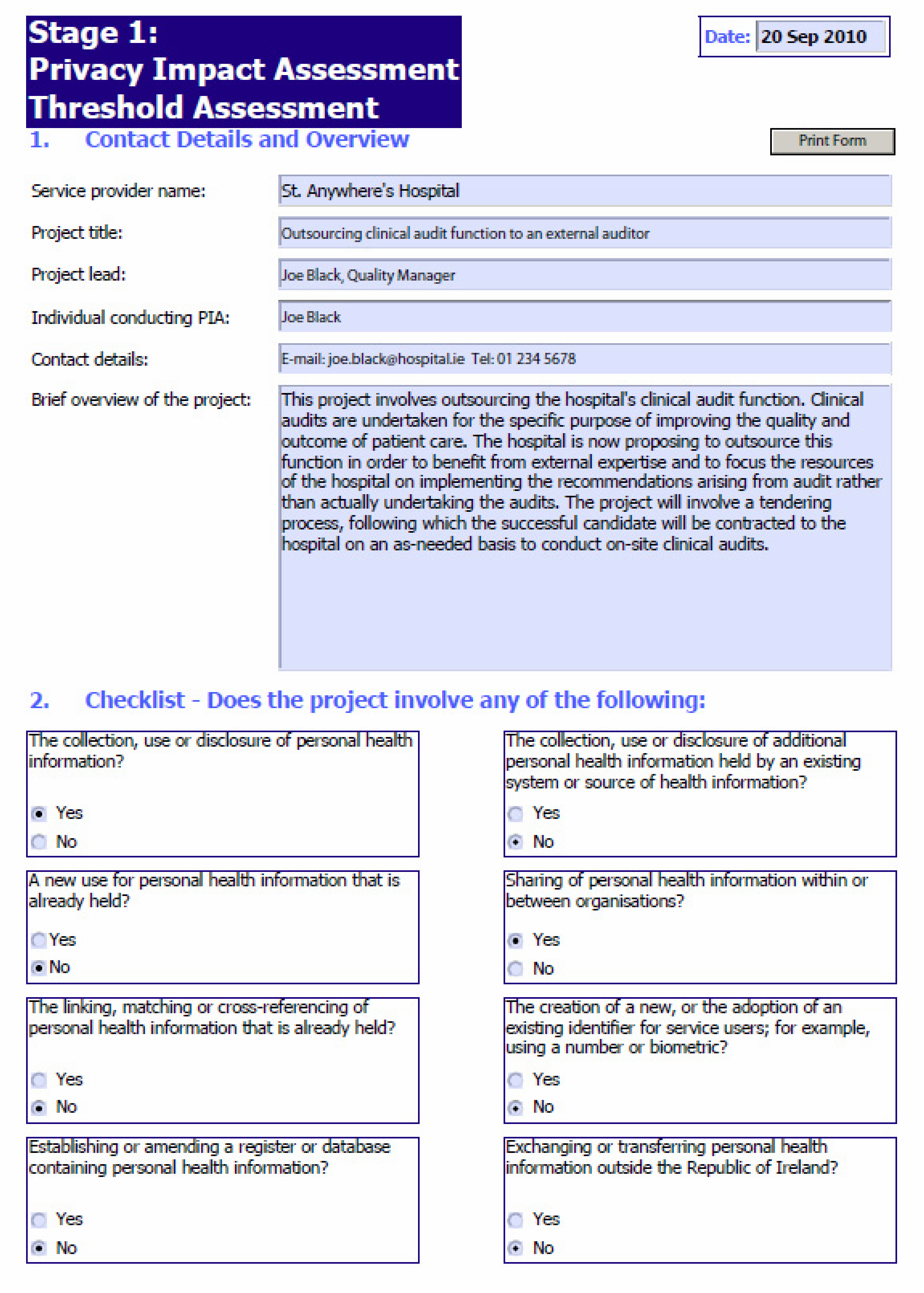
The external auditor will not have access to the hospital's patient administration system (PAS). Typically this may need to be accessed in the course of a clinical audit, for example to view results not yet in the medical record. The external auditor will instead be assigned a contact person who is a member of the medical records staff, who will access the necessary records on the PAS system as appropriate. The information that is required is then passed on to the auditor.

The project can be described as an add-on to an existing process. As such this PIA does not explore privacy risks associated with clinical audit or the clinical audit process that is currently in place in the hospital. Based on this, the PIA documented in this report focuses only on the access of an external auditor to patient healthcare records for the purpose of clinical audit and the associated security arrangements.

The project will involve a tendering process, in line with procurement guidelines, following which the successful candidate will be contracted to the hospital on an as-needed basis to conduct on-site clinical audits. Clinical audits will continue to be conducted in the same manner as previously, but by external auditors.

2. Stage 1 – Threshold Assessment

As a first step the project team completed a PIA threshold assessment (the threshold assessment is appendix 1 of this report). The project raises a number of issues around privacy, for example it involves a changed system of data handling in that the auditors accessing and analysing the personal health information will not be members of the hospital staff. The outcome of the threshold assessment as shown on the next page, was that it would be necessary to proceed with the PIA.



Stage 1: Privacy Impact Assessment Threshold Assessment

Date: 20 Sep 2010

Print Form

1. Contact Details and Overview

Service provider name: St. Anywhere's Hospital

Project title: Outsourcing clinical audit function to an external auditor

Project lead: Joe Black, Quality Manager

Individual conducting PIA: Joe Black

Contact details: E-mail: joe.black@hospital.ie Tel: 01 234 5678

Brief overview of the project: This project involves outsourcing the hospital's clinical audit function. Clinical audits are undertaken for the specific purpose of improving the quality and outcome of patient care. The hospital is now proposing to outsource this function in order to benefit from external expertise and to focus the resources of the hospital on implementing the recommendations arising from audit rather than actually undertaking the audits. The project will involve a tendering process, following which the successful candidate will be contracted to the hospital on an as-needed basis to conduct on-site clinical audits.

2. Checklist - Does the project involve any of the following:

The collection, use or disclosure of personal health information?

● Yes
○ No

A new use for personal health information that is already held?

○ Yes
● No

The linking, matching or cross-referencing of personal health information that is already held?

○ Yes
● No

Establishing or amending a register or database containing personal health information?

○ Yes
● No

The collection, use or disclosure of additional personal health information held by an existing system or source of health information?

○ Yes
● No

Sharing of personal health information within or between organisations?

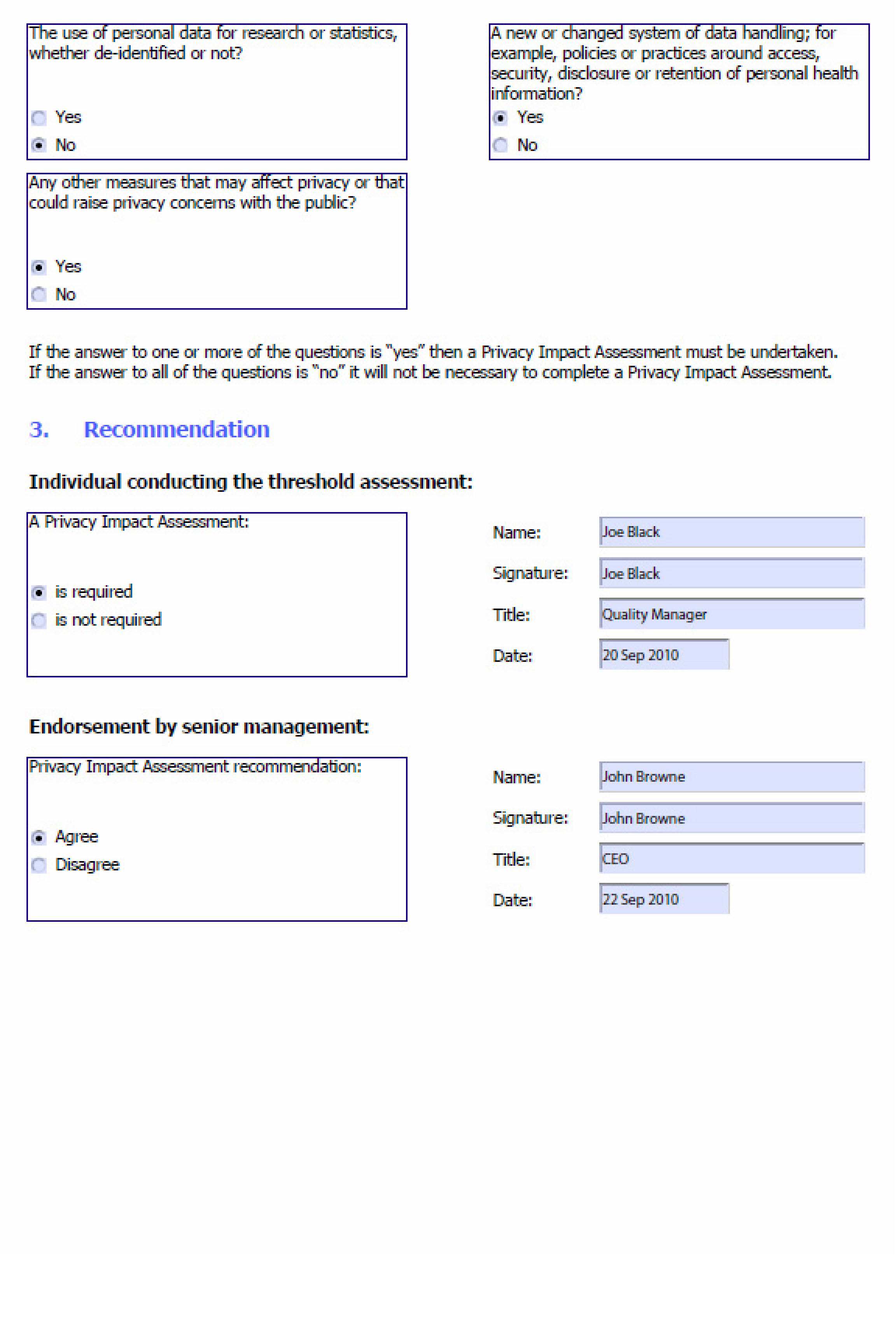
● Yes
○ No

The creation of a new, or the adoption of an existing identifier for service users; for example, using a number or biometric?

○ Yes
● No

Exchanging or transferring personal health information outside the Republic of Ireland?

○ Yes
● No



The use of personal data for research or statistics, whether de-identified or not?

○ Yes
● No

A new or changed system of data handling; for example, policies or practices around access, security, disclosure or retention of personal health information?

● Yes
○ No

Any other measures that may affect privacy or that could raise privacy concerns with the public?

● Yes
○ No

If the answer to one or more of the questions is "yes" then a Privacy Impact Assessment must be undertaken.
If the answer to all of the questions is "no" it will not be necessary to complete a Privacy Impact Assessment.

3. Recommendation

Individual conducting the threshold assessment:

A Privacy Impact Assessment:

● is required
○ is not required

Name:	Joe Black
Signature:	Joe Black
Title:	Quality Manager
Date:	20 Sep 2010

Endorsement by senior management:

Privacy Impact Assessment recommendation:

● Agree
○ Disagree

Name:	John Browne
Signature:	John Browne
Title:	CEO
Date:	22 Sep 2010

3. Stage 2: Identification of risks

The outcome of the PIA threshold assessment was to proceed to Stage 2 of the PIA. Stage 2 of the PIA process involved an exploration of the following:

- privacy management in the hospital
- a description of the project
- the project type and stage of development
- the scope of the project
- the information flows.

3.1 Privacy management in the hospital

In relation to privacy management, Table 1 outlines the stage of development of various policies and practices around privacy within the hospital. Although there is a statement of information practices in place this will need to be updated to reflect the changes to the clinical audit process to inform service users that this will potentially involve external auditors having access to their personal health information.

Table 1 - Privacy management in the organisation

Question	Yes	No	In Progress
Is there a privacy policy in place?	✓		
Is there a statement of information practices?	✓		
Is the hospital compliant with the principles of data protection?	✓		
Is there a records management policy in place that includes a retention and destruction schedule?			✓ (This is currently in the process of being updated – due for completion in November 2010)
Are administrative, technical and physical safeguards in place to protect personal health information against theft, loss, unauthorised use or disclosure and unauthorised copying, modification or disposal?	✓		
Is there an appointed privacy or information governance contact person?	✓		
Is there a privacy breach management action plan in place?	✓		
Are employees or agents with access to personal health information in the organisation provided with training related to privacy protection?	✓		

3.2 Project description

A detailed project description, project type and stage of development are clearly described in section 1 of this report – no privacy risks were identified in this regard.

3.3 Scope of the project:

Table 2 addresses questions around the scope of the project and any associated risks identified. This section explores the scope of the project with particular emphasis on the use of personal health information and why it is necessary. A series of questions are asked and the answers reflect the processes and safeguards that are in place to protect the privacy of service users' information. The final column in the table outlines potential privacy risks associated with each aspect.

Table 2 – scope of the project

Question	Answer	Privacy Risk
What information is proposed to be collected?	No additional information will be collected. The only change in practice will be that an external auditor will now have access to personal health information that has already been collected, for clinical audit purposes. The external auditor will have access to patient healthcare records in order to conduct the clinical audit. As such they will have access to personal details about the patient and their clinical information.	The external auditor undertaking the audit may use the information inappropriately or disclose it to another individual.
Outline why each element of the dataset is necessary.	The external auditor will need to assess the care provided to patients and decisions made – this information will often only be available on the patient healthcare record and as such this will be the source of information for clinical audit.	The auditor may know the individual service user in which case the service user may not be comfortable with them having access to such personal information as it is not strictly necessary for their care.

Question	Answer	Privacy Risk
Are the data subjects aware of the proposed collection, use and disclosure of their personal information? Identify and describe what information is given and how it is given.	The uses of health information are outlined in the hospital's statement of information practices, which is clearly displayed throughout the hospital.	Service users may not be aware that an external auditor may have access to their healthcare records for clinical audit purposes.
Have the data subjects consented to their personal information being used in this manner? Describe the consent process.	No - service users are aware that their information is used for clinical audit purposes but up to now this has been conducted in-house. It is proposed that the hospital will update their statement of information practices to reflect that clinical audit may now be conducted externally. This informs the service users of the practice.	Service users not aware that an external auditor may have access to their records for clinical audit purposes.
Identify and describe: ▪ All the uses of the personal information ▪ How these uses relate to the purpose for which the information was collected ▪ Any changes to the purpose for using the information after the information is collected ▪ Measures in place to prevent use for secondary purposes	The only change is that the personal health information will be accessed by an external auditor. The purpose is the same but the function will now be carried out externally. Access to personal health information by the auditor will be carried out in a controlled environment – in the healthcare records library with healthcare records being signed in and out as required (an audit trail will be kept). Further, the contract to be signed by the external auditors will include strict provisions that the data is not to be used for secondary purposes.	The external auditor using the information for purposes other than clinical audit.

Question	Answer	Privacy Risk
Identify and describe any potential sharing of the information and how the data subject has been informed of this.	This project does not involve information being shared with another organisation but will involve an external auditor potentially having access to patient healthcare records for clinical audit purposes. Service users will be aware of this possibility through the hospital's statement of information practices which is clearly displayed throughout the hospital. The results of clinical audits will be published but the data will be de-identified prior to this.	None identified.
Is it a possibility that the information will be linked or matched with an existing or proposed system? If yes please provide details	No	None identified.
Does the project, system or initiative involve assigning or using an identifier or using an existing identifier for a new purpose?	The service user's MRN is used as an identifier. Once the relevant data has been entered onto the computer for analysis service users will be identified only by their MRN. This process is the one which is currently in place, but the process will now be undertaken by external auditors.	None identified.

3.4 Information flows

The flow of personal health information in the process of clinical audit will remain the same as they currently are outlined in section 1, and depicted in Figure 1 below, but the steps will now be undertaken by an external auditor.

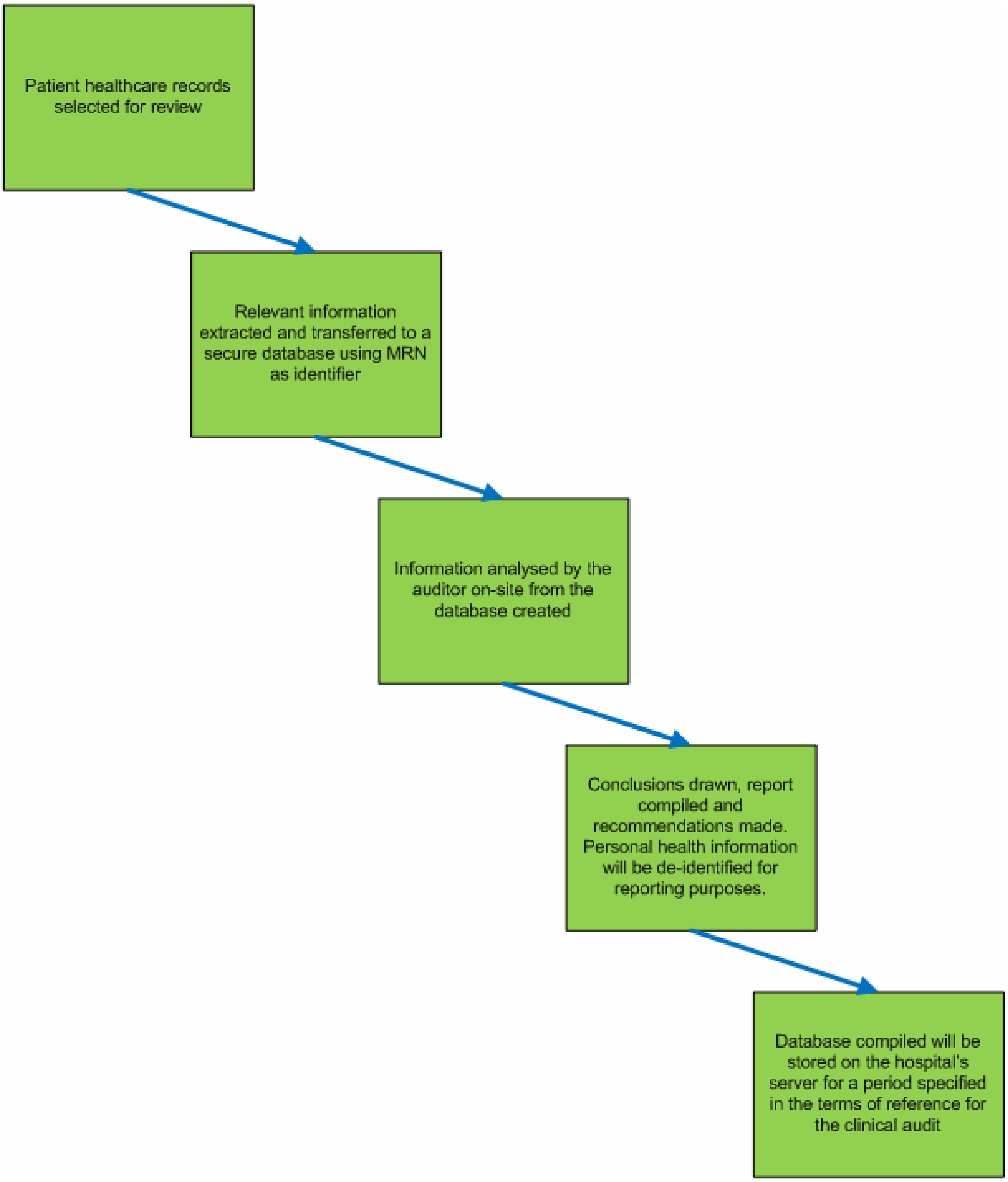

Patient healthcare records selected for review
Relevant information extracted and transferred to a secure database using MRN as identifier
Information analysed by the auditor on-site from the database created
Conclusions drawn, report compiled and recommendations made. Personal health information will be de-identified for reporting purposes.
Database compiled will be stored on the hospital's server for a period specified in the terms of reference for the clinical audit

Figure 1 – clinical audit information flows

Table 3 addresses questions around the information flows involved in the project and any associated risks identified.

Table 3 – Project information flows

Question	Answer	Privacy Risk
How will the information be collected?	There is no change to the way information will be collected – additional people will have access to the information as per the conditions that will be stipulated in contract between the hospital and the external auditor.	None identified.
What are the proposed uses of the information?	Clinical audit.	None identified.
Will the information be disclosed? To who? What precautions are in place?	The only change to normal proceedings is that the external auditor will have access to personal health information – most likely through patient healthcare records. However the person undertaking the audit on behalf of the hospital will not owe the same duty of confidentiality to the data subject as they are not bound by the same code of professional ethics. As such, confidentiality contracts will be signed that confer the same duty of confidentiality owed by health professionals on the external auditors. Further, the safeguards guaranteed by the successful candidate will form part of the decision in the tendering process.	The external auditor disclosing information about data subjects to another individual or organisation.
Will the data subjects have access to the information and have the opportunity to have any information about them corrected?	Not relevant – part of the wider functions of the hospital – it does not relate specifically to this project.	None identified.

Question	Answer	Privacy Risk
What security measures will be taken to protect the information from loss, unauthorised access, use, modification, disclosure or other misuse, including how data is transferred from sites?	The hospital's security policy sets out the practices and procedures that are in place to protect personal health information from unauthorised access, use, modification or disclosure. This includes measures to protect information as it is being transferred to other organisations – for example sending test results to GP practices. These will all apply to this project – however, the transfer of data policy will not apply as the information used in this case – patient healthcare records - will under no circumstances leave the hospital. However healthcare records will now be accessed by an external auditor. In order to ensure that additional records are not accessed unnecessarily and the records that are being reviewed for the audit are secure the following will apply: ▪ A log/audit trail of records will be kept detailing records signed in and out, when they are needed and the location of all records in use at all times ▪ All additional records not in use by the auditor will remain locked in their designated location ▪ When the auditor needs to access additional records or return them to the cabinet this will be done by a member of the hospital staff ▪ Data will be aggregated and analysed on one of the hospital's computers, which will be appropriately password protected. ▪ Information will be backed up to the hospital server.	Unauthorised access to sensitive information.
Identify and describe the retention and destruction practices to be employed in the project	The hospital's records management policy, which outlines retention and destruction practices, will be adhered to.	None Identified.

3.5 Risks identified

While exploring the aspects covered in Stage 2, a number of the risks were identified as similar and have been grouped together. The risks identified are:

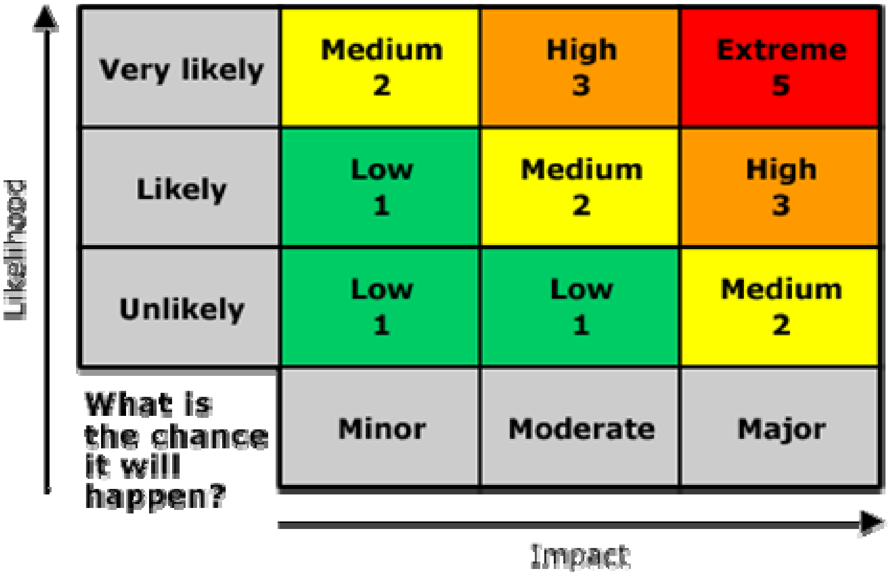
- medical professionals are bound by codes of conduct and owe a duty of confidentiality to service users. Each member of hospital staff has contractual obligations in relation to privacy. The external auditor may not be bound by these same codes of professional conduct, this may increase the risk of inappropriate disclosure of information
- due to change in practice the service users are not aware of proposed change in information practices and as such are not fully aware of how their information will be used. Service users have a right to know how their information is being used. Although implied consent is considered sufficient for clinical audit, service users need to be aware of this change in the clinical audit process and assured that appropriate safeguards to protect their privacy are in place
- the auditor may access additional patient healthcare records thereby accessing more personal health information than is necessary to complete the audit/unauthorised access to sensitive personal information. The risk in this instance is in relation to breach of access rights
- the auditor may use the information inappropriately, use it for secondary purposes or disclose it to another individual. Such misuse of information poses a risk to the privacy and confidentiality of service users and could result in the hospital being in breach of data protection legislation
- the auditor may know the service user whose record they are reviewing as part of the clinical audit process. Although this is a risk with the clinical audit process as it stands currently the service user could potentially be more uncomfortable with this proposal as the external auditor does not owe the same duty of confidentiality to the service user as a health professional.

4. Stage 3 – Addressing the risks

4.1 Analyses of risks

Figure 1 below is the risk matrix in use by the risk management team in St. Anywhere's. The use of the matrix enables risks to rated based on the likelihood that they will occur and the subsequent impact they would have. The rating of risks facilitates the appropriate management of risks, for example, if it is very likely that an event will occur and this would have a moderate impact the risk would be rated as high (number 3).

This matrix was used, in consultation with service users and staff, to analyse and rate the risks identified in Stage 2 of the PIA process, as represented in Table 4 below.



Very likely	Medium 2	High 3	Extreme 5
Likely	Low 1	Medium 2	High 3
Unlikely	Low 1	Low 1	Medium 2
What is the chance it will happen?	Minor	Moderate	Major

Likelihood
Impact

Figure 2 – Risk Matrix

Based on an evaluation of the likelihood of the risks occurring and the impact it would have the risks were rated as follows:

Table 4 – Risk Rating

Risk	Likelihood	Impact	Risk Rating
Medical professionals are bound by codes of conduct and owe a duty of confidentiality to service users. Each member of hospital staff has contractual obligations in relation to privacy. The external auditor may not be bound by the same codes of professional conduct; this may increase the risk of inappropriate disclosure of information.	Unlikely	Moderate	1= Low
Service users will not be aware of the change in information practices around clinical audit and that their personal health information may be accessed by an external auditor – this may be viewed by some as a violation of their privacy.	Unlikely	Moderate	1= Low
The auditor may access additional patient records thereby accessing more personal health information than is necessary to complete the audit/unauthorised access to sensitive personal information.	Unlikely	Major	2= Medium
The auditor may use the information inappropriately, use it for secondary purposes or disclose it to another individual.	Unlikely	Major	2= Medium
The auditor may know the service user whose healthcare record they are reviewing as part of the clinical audit process – service users may be uncomfortable with this.	Likely	Moderate	2= Medium

4.2 Addressing the risks

Having identified and rated these risks it was necessary to proceed to Stage 3 of the PIA. Stage 3 of the PIA process involves addressing the risks and identifying ways to mitigate or avoid them. This involved a consultation process with the staff of the hospital for their feedback and solutions and they were also asked to identify any further risks that could potentially arise as a result of this change in practice. The senior management of the hospital will be responsible for ensuring that these recommendations are implemented appropriately.

Table 5 sets out the risks identified and the actions put forward to address those risks.

Table 5 – Risks and proposed actions

Risk	Action put forward:	Person Responsible
Medical and nursing professionals are bound by codes of conduct and owe a duty of confidentiality to service users. Each member of hospital staff has contractual obligations in relation to privacy. The external auditor may not be bound by these same codes of professional conduct therefore there may be a risk that the auditor may disclose personal information.	Compose a legally binding contract of confidentiality to be signed by the auditor that is successful in the tendering process. This will detail in full the obligations of the auditor in terms of confidentiality and protecting the privacy of service users. Evaluation of tenders will take into account the ability to deal with sensitive and confidential information. This risk cannot be fully avoided but by putting this contract in place the risk is significantly reduced and provides the hospital with a means to manage the risk. The contract will place the same obligations on the external auditor as those conferred on health professionals by professional codes of practice.	Quality Manager to liaise with Legal Adviser around drawing up an appropriate contract. Quality Manager to brief Procurement Officer around tender requirements.
Service users will not be aware of the change in information practice around clinical audit and that their personal health information may be accessed by an external auditor – this may be viewed by some as a violation of their privacy.	Clinical audit is undertaken routinely in the hospital but patients need to be informed of this change in process – the change will be documented in the hospital's statement of information practices, which is clearly displayed throughout the hospital and on the hospital's website. The additional safeguards being put in place to protect privacy will be documented in this. The action put forward to address this risk will ensure that all service users will be aware, in as far as is practicable, of the change to the clinical audit process.	Information Manager and Patient Services Manager

Risk	Action put forward:	Person Responsible
The auditor may access additional patient healthcare records thereby accessing more personal health information than is necessary to complete the audit/unauthorised access to sensitive personal information	The following actions should be taken: ▪ Before each clinical audit is commenced the terms of reference and the information required will be clearly specified. This will form part of the contract between the hospital and the external auditors. The terms of reference will include the sample size of patient healthcare records that the auditor will need to access. These terms of reference will be upheld throughout the audit and the auditor will only have access to the patient healthcare records that are necessary to complete the audit. The auditor will work in the healthcare records library. Additional patient healthcare records will be stored there but the auditor will not have access to them ▪ An audit trail will be kept to track records signed out and returned. When the records are not in use they will be held securely ▪ The external auditor will not have access to the hospital's Patient Administration System (PAS). The external auditor will instead be assigned a contact person who is a member of the medical records staff, who will access the necessary records on the PAS system if required, for example lab results that have not yet been included in the paper records. The external auditors will be familiar with, and according to their contract adhere to, the hospital's security and records management policies. These security measures and limited access rights outlined above will act as additional preventions to the auditor accessing additional patient healthcare records and information that are not necessary for the purposes of the audit.	Quality Manager to produce terms of reference for each clinical audit as appropriate. Healthcare Records Manager to ensure an audit trail is kept of all records in use by the external auditors.

Risk	Action put forward:	Person Responsible
The auditor may use the information inappropriately, use it for secondary purposes or disclose it to another individual.	The following actions should be taken: ▪ The confidentiality contract discussed under risk 1 will act as a safeguard against this occurring ▪ The review of patient healthcare records will take place in the healthcare records library, which is physically secure. The healthcare records library can only be accessed by those with appropriate swipe cards. The number of auditors will be limited, with each receiving a "visitor access card" enabling them to access the healthcare records library for the duration of the audit. On completion of the audit the swipe cards will be immediately disabled. The records will not leave their designated area and will be locked securely away when not in use. This is in line with the hospital's security policy and will act as a deterrent to the information leaving the hospital thereby securing against inappropriate use. The possibility of this occurring poses a reputational risk to the hospital and could result in the hospital being in breach of data protection legislation. It is not possible to completely avoid this risk but the actions proposed will serve to mitigate both the likelihood and the consequences of the risk.	IT Manager

Risk	Action put forward:	Person Responsible
The auditor may know the service user whose healthcare record they are reviewing as part of the clinical audit process – service users may be uncomfortable with this.	In the course of discussions around this risk it was suggested that records selected for review could be de-identified or personal details blanked out leaving only the medical record number (MRN) as an identifier. However this would not be feasible for the hospital as the record may be needed to provide care to the service user at the time of the audit. Furthermore depending on the sample size it would be an incredibly onerous task for the staff of the hospital thereby defeating some of the purpose of undertaking this project. This risk cannot be avoided. However, the action outlined in response to risk 1 puts an onus on the auditor to act appropriately and maintain confidentiality. This should go some way towards reassuring the service user that confidentiality will be maintained and their best interests are being looked after. This risk is not so high that it will prevent the project from continuing as the potential benefits far outweigh the residual risk associated with it.	N/A

4.3 Residual Risks

Having completed Stages 1 - 3 of the process five risks were identified, four of which have been addressed. There is one outstanding risk as follows:

The auditor may know the service user whose record they are reviewing as part of the clinical audit process.

The solutions that were put forward to address this risk were not feasible. It is possible that the auditor may know the service user whose record they are reviewing and if the service user were aware of this connection they may feel that it is a violation of their privacy. Although clinical audit is currently undertaken routinely in the hospital with the distinct purpose of improving the quality of patient care, the fact that it will now be undertaken by an external auditor may pose a problem for some service users.

Although this risk cannot specifically be mitigated, the steps that will be taken by the hospital in addressing the other risks identified should go some way toward reassuring service users who may be concerned about it. For example the external auditors will be bound by the contract and service users will be aware of the possibility of their personal health information being used in this way.

4.4 Details of Consultation

Two consultations were held in the course of the PIA process in the form of focus groups of volunteers from the staff and a number of service users of the hospital. These consultations were undertaken in order to take account of the views and opinions of all parties to the process. Consultation forms an important part of conducting PIAs in that it offers the opportunity to gain fresh perspective and insights into the potential risks, how they can be addressed and the potential reaction to the particular undesirable event occurring which threatens the privacy and confidentiality of personal health information.

The first meeting of the group took place when Stage 2 of the PIA had been completed by the project team – identification of risks. The project team explained the details of the project and the progress so far in the PIA process. This meeting focused on identifying any additional risks that had not arisen during the exploration of the issues and completion of Stage 2 of the PIA process. No additional risks were identified at this meeting.

At the second meeting of the focus group the project team presented each risk that had previously been identified for discussion. The probability of each event occurring and its potential impact on both the service user and the hospital were discussed and rated using the hospital's risk matrix. Potential solutions and actions to mitigate or eliminate the risk completely were then put forward. The options were discussed at length, agreement was reached and a course of action decided upon.

A draft of this report (Stage 4 of the process) was circulated to those who had participated in the focus groups for their comments. The specific questions asked of them were:

- does the report accurately reflect the steps that were undertaken in the PIA process?
- have each of the risks that were identified been appropriately addressed?

The feedback on the report was positive with all of those involved acknowledging that the risks had been addressed and that the report accurately reflected the PIA undertaken by the project team. All comments were duly noted and incorporated into the report as appropriate.

5. Recommendations

Having completed the PIA the project team recommend that a number of actions be taken to uphold the privacy rights of service users. These actions combined serve to mitigate the risks identified in the course of the PIA. The actions required are:

- that the tendering process is thorough and robust and the successful candidate can demonstrate its ability in this area and can demonstrate its ability and competence in dealing with sensitive and confidential information
- a legally binding contract of confidentiality is put in place between the hospital and the external auditor that details in full the obligations of the auditor in terms of confidentiality and protecting the privacy of service users. This will place the same duty of confidentiality on the external auditor as those conferred on health professionals by professional codes of practice
- that the hospital's statement of information practices is updated to include this change to the clinical audit process, thus keeping service users informed of the way in which the hospital uses their information
- clear terms of reference are set for each clinical audit, indicating the information that will be necessary to complete it, with particular emphasis on the need to access patient healthcare records. These terms of reference will be adhered to for the duration of the audit
- the audit takes place in the healthcare records library and a process is developed whereby the auditor only has access to the records necessary to complete the audit. An audit trail will be kept to track records signed put and returned. When the records are not in use they will be held securely. The records will not leave the healthcare records library at any point.
- the external auditor will not have access to the hospital's Patient Administration System (PAS). Typically this may need to be accessed in the course of a clinical audit, for example to view results not yet in the medical record. The external auditor will instead be assigned a contact person who is a member of the medical records staff, who will access the necessary records on the PAS system as appropriate.

6. Endorsement by senior management of the organisation

The information detailed in this report is an accurate reflection of the project; the associated risks and the PIA process that was undertaken to identify and mitigate these risks.

The recommendations put forward in this report will be implemented prior to the commencement of the project and the measures will continue to form a part of the policies and processes of the hospital in the best interests of protecting the privacy of service users.

PIA and report completed by:

Signature: Joe Black

Title: Quality Manager

Date: 06/10/2010

Endorsement by senior management:

Signature: John Browne

Title: CEO

Date: 11/10/2010