Southern Health NHS Foundation Trust

Data protection audit report

ico.
Information Commissioner's Office

Auditors:	Claire Chadwick (Team Manager) Maria Dominey (Team Manager)
Data controller contacts:	**Lesley Barrington (Head of Information Assurance)** **Lisa Franklin (Director of Information and Technology)**
Distribution:	
Date of first draft:	5 November 2015
Date of second draft:	25 November 2015
Date of final draft:	11 December 2015
Date issued:	**11 December 2015**

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Southern Health NHS Foundation Trust.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report; however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

Contents

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 Southern Health NHS Foundation Trust (SHFT) has agreed to a consensual audit by the ICO of its processing of personal data.

1.4 An introductory meeting was held on 11 August 2015 with representatives of SHFT to identify and discuss the scope of the audit and subsequently to agree the schedule of interviews.

2. Scope of the audit

2.1 Following pre-audit discussions with SHFT, it was agreed that the audit would focus on the following areas:

a. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation. The scope has been amended to include third party contracts.

b. Subject access requests - The procedures in operation for recognising and responding to individuals' requests for access to their personal data.

3. Audit opinion

3.1 The purpose of the audit is to provide the Information Commissioner and SHFT with an independent assurance of the extent to which SHFT, within the scope of this agreed audit is complying with the DPA.

3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Reasonable Assurance	There is a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA. We have made one reasonable and one limited assessment where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report.

4. Summary of audit findings

4.1 Areas of good practice

SHFT have developed a process which allows the Information Governance Team to have effective oversight of the Information Asset Registers owned by the various Information Asset Owners in place throughout SHFT. Details of the process have been documented in a formal procedural document and an accompanying handbook provides further guidance.

There is a programme of regular spot checks conducted by the Information Governance Team. The checks involve physical site visits and interviews with staff, and are often conducted as a result of security incidents or in areas where high level information risks have been identified. Lessons learned are disseminated across SHFT.

There is an Access to Records procedure in place which gives guidance on dealing with Subject Access Requests (SARs). There are specific staff allocated to deal with the requests and to deal with any queries.

4.2 Areas for improvement

Although there are Information Asset Owners in place throughout SHFT, some are not sufficiently senior, with some having further delegated their responsibilities to their Information Asset Administrator.

SHFT do not conduct regular audits or checks to gain assurance that security clauses in third party data processor contracts are being adhered to, and that all SHFT policies are being followed.

Information requests are not differentiated to report on SARs and other requests separately and numbers are only collated biannually, as a result compliance with principle 6 of DPA cannot be monitored effectively.

Not all staff who process SARs have had sufficient training on how to apply exemptions to the DPA effectively.

5. Audit approach

5.1 The audit was conducted following the Information Commissioner’s data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

5.2 The audit field work was undertaken at Trust HQ (Tatchbury Mount), Romsey Community Hospital, Tom Rudd Unit, Moorgreen Hospital, Barton Park, Parkway Centre Havant, and Lymington Hospital between 20 and 22 October 2015.

5.3 In addition to the on-site visit the ICO ran two online staff surveys for 2 weeks, the first aimed at general staff and their awareness of Subject Access Requests, the second aimed at Access to Records Leads (ARL) and their understanding of the roles. There were 57 responses to the general survey from a total staff of approximately 7000 which is a response rate of less than 1%, therefore themes from this survey should be taken in this context. The ARL survey had a response rate of 37.5% (18 out of a total of 48 ARLs). Results from the survey have fed into the detailed findings in section 7.

6. Audit grading

6.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the following definitions.

Colour code	Internal audit opinion	Recommendation priority	Definitions
🟩	High assurance	Minor points only are likely to be raised	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non compliance with the DPA.
🟨	Reasonable assurance	Low priority	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA.
🟧	Limited assurance	Medium priority	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA.
🟥	Very limited assurance	High priority	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

7. Detailed findings and action plan

7.1 Scope A: Data Protection Governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

Risk: Without a robust governance process for evaluating the effectiveness of data protection policies and procedures there is a risk that personal data may not be processed in compliance with the Data Protection Act 1998 resulting in regulatory action and/or reputational damage.

a1. SHFT has a suite of Data Protection (DP)-related policies in place, which are overseen and monitored by the Information Governance Group (IGG). Policies include an Information Governance (IG) Policy, ICT Security Policy and a DPA Caldicott and Confidentiality Policy.

a2. All policies were up-to-date at the time of audit, and subject to regular review, although most are only subject to formal review every three years.

Recommendation: Review key policies on an annual basis if possible, or every two years as a maximum, to ensure content is appropriate and up-to-date.
Management response: Accepted
Owner: Lesley Barrington
Date for implementation: Define the key policies – then incorporate annual review via the policy schedule. March 2016.

a3. The IGG hold a log of policies which allows them to monitor review dates and to ensure that any necessary updates are carried out and updated versions are made available to staff by publication on the SHFT website, which ensures that staff will always be accessing the most recent and up-to-date versions.

a4. SHFT have a formal policy on Policy Management and a documented process for sign off of new policies which are approved by the IGG and presented to the Strategic Management Board for ratification and final sign off.

a5. Staff are advised of new and updated IG policies by line managers and in the Information Assurance (IA) newsletters which are published after IGG meetings to ensure key messages are highlighted and disseminated. The newsletters are published on the website.

a6. The IA Team also take steps to improve on or amend any policy or procedure where they have found that there is a lack of understanding amongst staff; for example, by analysing trends in security incidents.

a7. Trust staff contracts require all employees to comply with IG policies and procedures, although staff do not have to sign to say they have read and understood IG policies. Signed copies of contracts should be returned to HR; however this is not currently monitored and there are no checks in place to ensure this is done by all staff.

Recommendation: Implement a means by which the Trust can gain assurance that all contracts have been read, signed and returned accordingly.
Management response: Accepted.
Owner: HR IG Lead
Date for implementation: HR Department to review process and audit. April 2016.

a8. The IA Team sits within the Technology Directorate of the Trust, and is overseen by the Head of IA who reports to the Associate Director of Technology, who in turn reports to the Director of Technology (referred to informally as the 'delegated SIRO'), who reports to the SIRO who holds the position of Director of Finance.

Recommendation: Formally document the role of delegated SIRO, e.g. within the role profile and the Terms of Reference for the IGG.
Management response: Accepted.
Owner: Lesley Barrington
Date for implementation: March 2016

a9. The IGG is chaired by the delegated SIRO and the group feeds into the Informatics Forum which is attended by the SIRO. The SIRO does not attend the IGG but receives a summary and selected key issues via this route. The Terms of Reference for the IGG however state that the SIRO attends the meetings, and there was conflicting evidence regarding who chairs the Informatics Forum.

Recommendation: a) Update the Terms of Reference for the IGG to state that it is chaired by the delegated SIRO, rather than the appointed SIRO.
b) Update the Terms of Reference for the Informatics Forum if this is chaired by the SIRO rather than the Caldicott Guardian.
Management response: Partially accepted. a) IGG TOR to be checked and updated. b) Informatics Forum TOR checked and is chaired by the SIRO.
Owner: Lesley Barrington
Date for implementation: March 2016

a10. The details of the SIRO's and delegated SIRO's roles are not set out formally, although the Director of Finance's job description does refer to the role. The delegated SIRO was not available for interview in order to obtain evidence of her duties and responsibilities.

Recommendation: Formalise the key responsibilities for each role by documenting these in a written format, for example, the 'Roles and Responsibilities of the IG Leads' document.
Management response: Accepted.
Owner: Lesley Barrington
Date for implementation: March 2016

a11. The Head of IA also line manages the IG Manager, Records Manager, and the ICT Security Specialist whose role is primarily to give advice on Information Security (IS) issues and provide technical support when required. The ICT Security Specialist also attends the IGG.

a12. Other key roles include the nominated Records Leads and IG Leads, who sit within each service area and have IG and records management responsibilities for their respective teams, and the Caldicott Guardian who has primary responsibility for data sharing with other organisations as well as overall responsibility for SHFT's compliance with the DPA.

a13. The IGG meet every two months and the group acts as a forum for the discussion of key IG, IS and DP issues. The agenda for the group is built around the IG Toolkit requirements.

a14. Some policies, although up-to-date in their review cycle, contain out-of-date job titles such as the IA Manager and IS Advisor.

Recommendation: Update all out-of-date job titles in policy, including the DPA Caldicott and Confidentiality Policy to refer to the ICT Security Specialist not the IS Advisor, so that staff are aware of current governance structures. Also replace references to the IA Manager with the Head of IA in the Information Risk Management Policy.

Management response: Accepted.

Owner: Lesley Barrington

Date for implementation: Will be completed as per a2 – review of policies schedule March 2016

a15. There is an Information Risk Management Policy in place which clearly sets out the SHFT's process for managing information risks, and which is monitored for compliance by the IGG. The ICT Security Policy refers to the method used for incident reporting i.e. via Ulysses, and this refers to risk management procedures.

a16. SHFT uses the Ulysses system as its risk management and incident reporting tool. The risk registers are stored on this system, including the overarching Corporate Risk Register, divisional risk registers (including a Technology register) and individual project risk registers.

a17. Information risks can originate from a number of sources and can easily be added to the most appropriate risk register which may be in a local area. The IGG members can bring identified risks for further discussion to the IGG meetings and where appropriate, risks can then be further escalated via the Informatics Forum to the SIRO and then potentially to the Board for consideration for the Corporate Risk Register. An example of a DP-related risk was noted on the Corporate Risk Register observed by auditors.

a18. In addition, the IG Leads receive monthly risk reports from Ulysses which they use to help to grade IG-related risks, and can take relevant risks to the IGG. The SIRO also receives a copy of this report.

a19. The IG Facilitators manage the Information Asset Register (IAR) process. Due to the large number of services across SHFT, each area has a local IAR and IG retains oversight of these using a documented process. This process was developed by IG following an extensive data mapping exercise.

a20. Although individual IARs are the responsibility of Information Asset owners (IAOs) within each service area/team, IG provide support and monitor the registers to ensure they are managed correctly and risks are reviewed regularly.

a21. Details of the process have been documented in a formal procedural document and in an IAO and Information Asset Administrator (IAA) Handbook which is provided to all IAOs and IAAs.

a22. The IG Team record higher level risks on a separate spreadsheet for closer monitoring. These risks will be reviewed more frequently.

a23. The log details any recommendations made by IG in relation to the risks which are tracked and followed up if not actioned in line with set timescales.

a24. As a further control, IG send reminders to IAOs two months before their risk reviews are due. The regularity of reviews depends on their ratings. Reviews can be done annually, every six months or monthly.

a25. IG also prepare a summary report in advance of IGG meetings to help keep the delegated SIRO and IG Leads updated. However, there was no evidence that this information is fed to the SIRO via the Informatics Forum or via another route.
Recommendation: See a9. It would be good practice to feed the summary report to the SIRO either via the Informatics Forum or similar appropriate route.
Management response: Accepted.
Owner: Lesley Barrington
Date for implementation: Review of the Informatics Forum TOR already being completed. Standard reporting proforma from IGG will be updated to include IA Management Report. March 2016.

a26. Some IAOs are at a senior level within SHFT, however others were the equivalent of team manager level, and some had delegated their responsibilities to their IAA.

Recommendation: Where possible, assign the IAO role to senior management roles within the Trust in order to ensure that responsibility for information assets sits at an appropriately senior level. Operation responsibilities can still be delegated to an IAA but this role should also be reasonably senior (e.g. line manager level).
Management response: Accepted
Owner: Sharon France
Date for implementation: Review of IA Management structure to be completed – due to the size and complexity of the Trust this will be incorporated into the IG Workplan for 2016-17. Implementation will include the requirement to complete on-line training.

a27. Although there is plenty of guidance and support available, IAOs interviewed were not able to demonstrate an understanding of the purpose and requirements of their role.

Recommendation: See a26. See above.

a28. SHFT have implemented a Privacy Impact Assessment (PIA) Procedure and associated guidance for staff use. The guidance is based on the older version of the ICO's PIA guidance, and is authored by the Head of IA. The procedure sits under the DPA Caldicott and Confidentiality Policy.

Suggestion: Update the procedure to reflect advice contained within the current ICO Code of Practice.

a29. IG maintain a PIA log of those PIAs which are brought to their attention, but are aware that they are not always consulted in all projects which may require some form of PIA (including the sharing of data with other organisations), despite this being a policy requirement.

Recommendation: The Trust should implement further means of ensuring that PIAs are undertaken where necessary. For example, include a standard checklist in relevant policy documents which includes the requirement to conduct a PIA if a system/procedure that involves processing personal data is being implemented or revised.
Management response: Accepted.
Owner: Lesley Barrington
Date for implementation: To be incorporated into the IG Workplan for 2016/17. Will require engagement with SHFT Policy Management Team.

a30. Some controls are in place to enable PIAs to be considered when necessary, such as technical projects where the Head of IA and the ICT Security Specialist are consulted for advice; however the Procurement team's new contracts process does not include a formal requirement to check with IG regarding a PIA, and the Trust has recognised that this is a weakness which has led to IG being left out of the loop on occasions. Furthermore, procurement staff do not have sufficient DP knowledge to recognise the potential for a PIA on every occasion.

Recommendation: See a29. Update Procurement's processes to require them to consider the need for a PIA in every case.
Management response: Accepted.
Owner: Sharon France and Head of Procurement
Date for implementation: To be incorporated into the IG Workplan 2016/17.

a31. PIAs brought to the IGG are signed off there by the membership and the Chair.

a32. The DPA Caldicott & Confidentiality Policy contains a requirement for SHFT to ensure that arrangements with third parties who process personal data on behalf of the Trust are subject to a written contract which stipulates appropriate security and confidentiality clauses.

a33. All SHFT contracts use the standard NHS terms and conditions which include IG clauses. Contracts observed during the audit included DP and security clauses.

a34. SHFT main log of third party contracts is held centrally by Procurement, on the Bravo system. SHFT acknowledged that the log is not yet complete but work is progressing to ensure that all data processor contracts are eventually entered onto the log.

Recommendation: Complete the log with all third party contracts involving personal data and implement a process to ensure all new contracts entered into in the future will also be included.

Management response: Accepted.
Owner: Sharon France and Head of Procurement
Date for implementation: March 2016

a35. Individual contracts are the responsibility of Contract Managers within divisions. Monthly meetings are held with the Contract Managers, Procurements and the third party contractors to review set KPIs including checks on numbers of security incidents.

a36. There are no regular audits or checks made by Procurements or Contract Managers to gain assurance that security clauses in third party contracts are being adhered to, and that all SHFT IG policies are being followed.

Recommendation: Conduct regular (at least annual) checks of third party processes to assess their compliance with Trust policies, contracts and the DPA. This can be done using a risk-based approach (e.g. depending on the volume and sensitivity of personal data processed), with higher level risks being audited more frequently than lower level ones.
Management response: Accepted.
Owner: Sharon France
Date for implementation: To be incorporated into the IG Workplan 2016/17.

a37. The IGG reviews SHFT's compliance with IG training, and numbers and details of security incidents, in each meeting. The IG Leads provide updates from their service areas and the IG Manager provides a detailed breakdown of security incidents including trends and significant incident details, for discussion and action planning. Requests for personal data are reported twice a year, although the format does not currently clearly demonstrate SAR compliance.

Recommendation: See b49

a38. IG is not included in the annual Internal Audit plan. However, the requirement for IG audits to be undertaken is documented in relevant policies and job descriptions. The current process for this is a programme of regular spot checks which involve physical site visits and interviews with staff based there. The checks are completed as part of a 3 year rolling programme and are conducted by the IG Team and can be (and often are) conducted as a result of security incidents or conducted in areas where high level information risks have been identified.

a39. The IG Team are required to do four spot checks per month which can be linked to identified information risks. This is a team KPI. IG Leads also conduct ad hoc spot checks when possible within their respective areas.

a40. IG help to disseminate lessons learned from the checks, and share good practice across teams within SHFT, during the course of these onsite visits.

7.2 Scope B: There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.

Risk: Without appropriate procedures there is a risk that personal data is not processed in accordance with the rights of the individual and in breach of the sixth principle of the DPA. This may result in damage and/or distress for the individual, and reputational damage for the organisation as a consequence of this and any regulatory action.

b1. SHFT has a policy in place for the processing of requests titled Access to Personal/Clinical Records Procedure.

b2. This policy has been produced by the Records Manager and is regularly reviewed with the latest version due to be approved and published in the near future. The policy is available to staff via the internet.

b3. There is a leaflet in place for the public, which is available in paper form and on the SHFT website. It refers to the 40 day timescale, however, it does not contain a contact name or address to send the request to or mention the fee or need for identification.

Recommendation: In order to be fit for purpose the leaflet on requests should include a point of contact to make requests to, and link to application form for more information.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: March 2016

b4. There is an application form for requests that does refer to details above and gives the Records Manager as point of contact.

b5. Information on making a subject access request may be considered difficult to locate as it can only be found via a search at present rather than via a direct link.

Recommendation: Add a direct link to information governance/SAR page in an easily located place on the website.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: March 2016

b6. Due to SHFT being the result of a merger between a mental health trust and a community trust there are two distinct procedures for the processing of requests.

b7. The services historically offered by the mental health side of the trust have Access to Records Leads (ARLs), who are based within the service, and the requests on the community side are dealt with centrally by one Subject Access Administrator (SAA), only the latter comes under the direct responsibility of the IA department.

b8. This procedure appears fit for purpose given that the nature of the mental health requests are more complex and will require additional support from the health care professional. Requests on the community side are more straightforward and often restricted to copies of scans etc.

b9. The SAA is a full time role and reports directly to the Record Manager, however the other ARL process requests for the service in addition to their formal role and no evidence was provided that it was documented in their job description.

Recommendation: In order to formalise the ARL role it should form part of staff's job description or as an appendix.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: Involves staff from other clinical services – will be incorporated into the Records Workplan 2016-17.

b10. There is a comprehensive list of all the ARLs in place; however this is maintained by the Records Manager and not easily accessible by all staff.

b11. The Records Administrator acts as the deputy to the SAA in their absence; this position is currently vacant and the IG Facilitator is providing some resilience, however this deputation is represented on the list.

b12. ARL sickness/holiday cover is in place in most cases and their contacts are also available on a central list; however there is no evidence that these staff have had specialist SAR training.

Recommendation: Ensure that there are adequately trained 'deputies' in place for all ARL (including SAA) to ensure that requests aren't delayed due to staff absence. Contacts details should be readily available to staff so they know who to forward requests to (perhaps add a link in the SAR procedure).
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: Involves staff from other clinical services – will be incorporated into the Records Workplan 2016-17.

b13. There is general IG training which is mandatory for all staff. However, although there is an exercise on identifying a Freedom of Information (FOI) request, this is under the FOI section of the training and does not clearly give guidance on how to identify a Subject Access Request (SAR) and how to action it. A link to the Access to Personal/Clinical Records Procedure is provided in the IG e learning.

Recommendation: It would be best practice to revise the training for general staff to highlight how to identify a SAR and who to refer it to in a timely manner, rather than relying on staff reading a lengthy procedure.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: March 2016

b14. 28% of respondents to the staff survey said that they would not recognise a SAR if they received one.

b15. There is training in place for the ARLs, the content of which is good. However not all relevant staff have received this, the SAA stated that they had not received it and its completion is not actively monitored.

b16. Although the definition of a SAR is documented in the Access to Personal/Clinical Records Procedure, on speaking to staff it was clear that clarification was needed over the difference between a SAR as defined by the DPA 98 and a disclosure of personal data as allowed by an exemption to the DPA 98, this is reflected in the survey where 83% respondents believed that a request from the police for information on a patient constituted a SAR.

b17. In addition some staff did indicate a lack of confidence in knowing which information should be redacted.
Recommendation: Ensure all ARL (inc SAA) have received specialist request training including differentiating between SARs and disclosures and correctly applying exemptions.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: Involves staff from other clinical services – will be incorporated into the training workstream on Records Workplan 2016-17.

b18. Although the policy applies across SHFT there are several differing procedures in place for the actual processing of SARs dependant on location, however core DPA 98 compliance is in place in all areas.

b19. Staff stated that they would confirm the identification of a requestor, with some stating that they would confirm address, however staff interviewed were not aware of defined list of accepted identification, although the Access to Personal/clinical Records Procedure does provide examples of what may be accepted.

Recommendation: Ensure all staff who process SARs are made aware of where this can be found.
Management response: Accepted
Owner: Rachel Lloyd
Date for implementation: Will be incorporated into Records Workplan 2016-17

b20. Some staff stated that they would contact the subject directly if a request was received via a third party, to check that their consent was valid and to check their understanding of the level of information requested; this is good practice in relation to a SAR.

b21. There are clear processes in place for when children/parents of under 18s make requests.

b22. Checks are made to ensure that suitable powers of attorney are in place if applicable. Guidance is in place to guide staff on the types of POA, SHFT may want to supplement this with recent guidance from the Alzheimer's society.

b23. Staff interviewed were all clear that the 40 days started from the date received at the Trust and if they required further clarification they would seek it promptly.

b24. Expectations were managed effectively if it was likely that the 40 days were going to be exceeded.

b25. There are local request logs in place, however there is no central oversight of these and SARs and disclosures are not differentiated, also the information recorded is not consistent between services. An explanation of the exemption applied when any information redacted is not recorded here.

Recommendation: Ensure all ARLs maintain a log of requests, differentiating between SARs and disclosures, clearly showing how many days SARs have taken to complete and documenting the exemptions applied for any information withheld. These logs should be held centrally to allow corporate oversight by the record manager.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: Will be incorporated into the Records Workplan 2016-17. Resources will be required to develop a secure Sharepoint site for all ARLs to document and log SARs and disclosures.

b26. There is a SAR Toolkit and checklists in place to ensure specific steps are taken when responding to a request, however these are not consistently used in all services and do not necessarily include all the stages needed to ensure compliance.

Recommendation: See b18.

b27. There are no weekly meetings to discuss SAR progress, however there are ARL forums held around every two months, used to discuss common issues.

b28. SHFT do have comprehensive information asset registers (IAR) in place, although at present they do not form part of the process to locate information for a SAR, mainly because ARL in post have been in the role for a long time and know where to look.

Recommendation: It would be good practice to encourage ARLs to use the IAR to ensure that all systems/locations have been checked in response to a request, especially for any new staff who take on the role.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: March 2016

b29. SHFT recently migrated to 'Open Rio' as their patient administration system. There is a facility to track the location of manual files. Historically there have been issues printing and extracting information from this system coherently, it is hoped that the move to Open Rio will have relieved this problem.

Recommendation: Encourage staff to feed back any issues with printing from Open Rio, to ensure any remaining issues can be addressed.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: March 2016

b30. Paper records are required to be stored chronologically within the file, however it was stated that there is no requirement for community files to be indexed or sectioned which may make information more difficult to locate, however these files are from other data controller and processed by SHFT to provide a streamlined service only.

b31. It is procedure to ensure emails are included within a request response, some Health Care Professionals (HCP) print off emails and store on record, others keep electronically.

b32. HR have two legacy systems where mental health managers store personnel files locally and community store centrally. With the former process it raises the risk that when staff change managers or a manager leaves the staff personnel file may not be passed on appropriately. It was reported that a move to a centralised model is proposed.

Recommendation: Consider centralising and indexing HR records, in addition to allowing easier access to information in the event of a SAR, it will also help compliance with the other principles of the DPA 98.
Management response: Accepted.
Owner: Rachel Lloyd / HR ARL
Date for implementation: Involves staff from other service – will be incorporated into the Records Workplan 2016-17.

b33. Most staff interviewed appeared to have good knowledge about the exemptions that could be applied when responding to a request.

b34. However there were some instances where staff lacked confidence that what they were withholding was correct.

Recommendation: See b15/b16/b17

b35. The definition of 'third party information' did not appear in all cases to be as defined by the DPA 98 and sometimes incorporated information provided by third party organisations.

b36. For example, information provided by the local council was said to be removed from requests, when this reason alone is not a valid exemption, however if the information was around safeguarding then its release may incur 'damage or distress' to the individual or a third party and so this exemption could be applied.

Recommendation: SHFT should ensure that guidance with the correct definition of third party data (see section 7 of ICO code of practice of SARs) is provided to ARLs.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: March 2016

b37. OpenRiO (Rio) has a tick box facility so that third party information can be highlighted with a patient record. However the whole section may not actually be third party information. It was reported that staff review this information to check this prior to release.

Recommendation: see b35/b36

b38. It was reported in most services that the HCP had final say in which information was withheld, despite the fact that they did not have formal data protection training.

Recommendation: If the HCP completes redaction ensure that the exemption being used when information is withheld is documented and the ARL should then check they are being applied correctly.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: Will be incorporated into the Records Workplan 2016-17, and in the development of centralised SAR log process on Sharepoint.

b39. There were differing procedures for redaction, including blacking out and copying, 'tippex mouse' and copying and requesting a third party solicitor complete this using redaction software.

b40. It is not common practice to document the reason for redaction.

Recommendation: The reason for redaction should be documented to allow for a clear audit trail in the event of a complaint – see b23/b24/b25.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: Will be incorporated into the Records Workplan 2016-17, and in the development of centralised SAR log process on Sharepoint.

b41. There was no evidence of quality assurance checks to ensure exemptions are being applied correctly and consistently.

Recommendation: Implement a programme of sip sampling on SAR responses to ensure exemptions are being applied correctly by ARL/SAA.

Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: Will be incorporated into the Records Workplan 2016-17, and in the development of centralised SAR log process on Sharepoint.

b42. Information is provided predominantly in paper form either sent recorded delivery or collected by the subject. If the subject requests information electronically then a letter outlining the risks is sent to the subject asking them to consent to the transfer.

b43. Covering letters differ between services with not all of them covering the requirements of section 7 of DPA 98.

b44. It is not common practice at SHFT to proactively inform the subject which exemption is being applied when data has been withheld.

Recommendation: Ensure that covering letters include all requirements of section 7 of the DPA 98.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: Will be incorporated into the Records Workplan 2016-17, and in the development of centralised SAR log process on Sharepoint.

b45. SHFT offer the facility for subjects to view their records onsite with the relevant HCP if it is felt that further support and clarification will be needed with the provision of the data.

b46. No explanation of abbreviations and codes is provided with the response.

Recommendation: SHFT should consider practical ways, such as website links to common abbreviations and options to contact ARL for clarification, to ensure that information provided is intelligible.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: March 2016

b47. Copies of the information disclosed are kept within the service for a period and retained for three years. The community requests are kept electronically although it was not clear if the same retention periods apply.

Recommendation: Ensure staff are aware that SAR copies retained electronically are only retained for three years as per the retention period.
Management response: Accepted
Owner: Rachel Lloyd
Date for implementation: Records Workplan 2016-17
Justification: Process is in place.

b48. It was reported that the KPI for SAR compliance is 100%. A SAR dashboard is in use which shows that 82% of requests so far this financial year have been fulfilled with 40 days.

b49. At the time of the audit the numbers of requests were escalated to the Records Manager bi annually who then presents to the IGG. Unfortunately the figures do not differentiate between SARs and disclosures and therefore cannot demonstrate the percentage of SARs completed within 40 days.

Recommendation: Reporting on compliance of SARs should be revised, clearly differentiating between SARs and disclosures. With the use of centralised logs (b23/b24/b25) the Information Assurance team with have clear ongoing oversight of compliance with principle 6.

Management response: Accepted.

Owner: Rachel Lloyd
Date for implementation: Will be incorporated into the Records Workplan 2016-17, and in the development of centralised SAR log process on Sharepoint.

b50. The reasons why requests have exceeded 40 days are documented, which is good practice to identify any areas of concern. However, due to the manner in which data is currently reported not all instances refer to definitive non-compliance.

Recommendation: When reporting to the IGG, the number of SARs should be separated from other requests and the number of these that have exceeded 40 days reported. It would still be useful to document why the 40 days have been exceeded and use the information to identify any trends and rectify them if possible, if not it would be good practice to highlight them as an information risk.
Management response: Accepted.
Owner: Rachel Lloyd
Date for implementation: Will be incorporated into the Records Workplan 2016-17, and in the development of centralised SAR log process on Sharepoint.

b51. If a subject is unhappy with a response, most services would endeavour to deal with the complaint themselves and if applicable would refer them to the Trust complaints department.

b52. It was reported that learning from SAR complaints is shared via the ARL forum and IGG group reporting

7.3 The agreed actions will be subject to a follow up audit to establish whether they have been implemented.

7.4 Any queries regarding this report should be directed to Claire Chadwick, Team Manager, ICO Audit.

7.5 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of working practices, policies and procedures. The following staff members were particularly helpful in organising the audit:

- Lesley Barrington (Head of Information Assurance)
- Rachel Lloyd (Records Manager)
- Sharon France (Information Governance Manager)