Tees, Esk and Wear Valleys
NHS Foundation Trust

Records management and safe haven

Ref CORP-0026-007-v1

Status: Approved
Document type: Procedure
Overarching policy: Records Management Policy

Contents

1 Purpose

Following this procedure will help the Trust to:-

- Maintain the privacy and confidentiality of personal information;
- Ensure compliance with legal requirements, especially concerning sensitive information (e.g. people's medical condition);
- Give confidence to Trust staff, other Trusts or other agencies that personal information is being sent to a location which ensures the security of data. It is therefore essential that all departments and services within the Trust put in place adequate safe haven procedures to protect information, specifically:

    - At the point of receipt.
    - Whilst held by the department.
    - When transferring information to others, by whatever means.
    - When archived.
    - At the point of disposal.

2 Objectives

This procedure provides:

- The legislative context and guidance which dictates the need for a safe haven
- A definition of the term safe haven
- When a safe haven is required
- The necessary procedures and requirements that are needed to implement a safe haven culture
- Who can have access and who you can disclose to

3 Related documents

- The Records Management Policy defines the legal duty to make sure records are managed and secure throughout their lifecycle.
- You must read and understand the Records Management Policy before carrying out the procedures described in this document.
- All staff are responsible for ensuring the protection of person identifiable information received into a safe haven.

This procedure also refers to:-

✓ Information Security and Risk Policy

- ✓ Information Asset Register Procedure
- ✓ Email policy
- ✓ Email procedure

4 Accessibility to safe haven area

Staff with a disability may have difficulty using safe havens if, for example the location of a safe haven fax makes it impossible for a disabled member of staff to physically access the machine. Should this occur, contact the information governance manager who will investigate and resolve the issue on an individual basis.

5 Where should safe haven procedures be in place?

- In any location where large amounts of personal information is being received held or communicated especially where the personal information is of a sensitive nature e.g. patient identifiable information.
- There should be at least one area following safe haven procedures on each of the Trust sites.

6 Legislation and Guidance

6.1 Data Protection Act 2018 (GDPR)

Article 5-1 (f) "*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*"

6.2 Department of Health NHS Confidentiality Code of Practice

Annex A1 Protect Patient Information - *"Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are as secure as they can be".*

7 Location/security arrangements

- It should be a room that is locked or accessible via a coded key pad only to authorised staff <u>OR</u>

- The office or workspace should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to any members of staff who work in the same building, or any visitors.
- If sited on the ground floor any windows should have locks on them.
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Manual paper records containing person-identifiable information must be stored in locked cabinets.
- Computers should not be left on view or accessible to unauthorised staff and be either locked (if you plan to return) or switched off when not in use. Files and folders should always be saved and closed to allow for back-ups to be taken or in case of unexpected downtime.
- Equipment such as fax machines in the safe haven should have a code password if possible and be turned off out of office hours where practical.

8 Fax machines

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so and there is no other secure method available (e.g. secure email). The use of a fax machine must be recorded on the team's information asset register so that the associated risks are identified and managed. For advice on safer ways of working with information, contact tewv.informationsecurity@nhs.net.

- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it.
- The sender is certain that the correct person will receive it and that the fax number is correct.
- You notify the recipient when you are sending the fax and ask them to acknowledge receipt.
- Care is taken in dialling the correct number (where possible programme numbers into fax memory to avoid misdialling).
- Confidential faxes are not left lying around for unauthorised staff to see.
- Only the minimum amount of personal information should be sent, where possible the data should be anonymised or a unique identifier used.
- Faxes sent should include a front sheet, which contains a suitable confidentiality clause and state the number of pages included in the transmission.

9 Communications by post

- If the internal mail system is being used to receive person identifiable or sensitive information, physical security measures, such as key coded or swipe card entry, must be in place to protect information in the post-room and post collection and delivery points.

• All sensitive records must be stored face down in public areas and not left unsupervised at any time
• Incoming mail should be opened away from public areas
• If the post (both internal and external) contains patient or staff information it should be sealed securely and marked “confidential”.
• Always send post to a named person and named team.
• The trust guidelines of a three line minimum address must be followed.
• If using a window envelope, ensure that the only information that is visible is the person’s name.

The Trust’s procedure for moving records and other sensitive information gives guidance on using the postal service for transferring information.

10 Communications by telephone

Recorded telephone messages containing person identifiable or sensitive information, e.g. the names and addresses of applicants phoning for a job, or patient details, must be received into a secured, PIN-code protected voicemail box, so that only those entitled to listen to the message may do so.

A deputy should be appointed for times of absence, a group PIN code issued or an administrator password made available. Some areas use a messages book to note messages for absent staff members, this should also be stored securely.

11 E-mail

Many e-mail systems (not NHSmail) are not secure which all staff are made aware of during induction training and training to use the NHSmail system.

Patient identifiable and other sensitive information must not be sent by e-mail unless it has been encrypted to standards approved by the NHS. See the Email Procedure to identify which email addresses are secure, and for advice on the Trust-approved approach to sending sensitive information to non-secure email addresses.

E-mails containing confidential information must be stored appropriately on receipt e.g. incorporated within the health record, and deleted from the e-mail system when no longer needed.

12 Sharing information with other organisations (non NHS)

Employees of the Trust authorised to disclose information to other organisations must seek an assurance that these organisations have a secure point for receiving personal information.

The Trust must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- Data Protection Act 2018 (GDPR)

- Common Law Duty of Confidence
- Department of Health NHS Confidentiality Code of Practice

Staff sharing personal information with other agencies should be aware that the Trust is a signatory to the *North East Information Sharing Guidelines* guidance which is applicable to all public sector organisations in the North East.

13 Definitions

Term	Definition
Safe haven	• "Safe haven" encompasses all secure methods of transmitting or transferring confidential information. • The term safe haven is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure person-identifiable information can be held, received and communicated securely.
Personal information	• Information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name and private address, name and home telephone number etc.
Sensitive information	Personal information which contains details of that person's: • racial and ethnic origin • offences and alleged offences • criminal proceedings, outcomes and sentences • trade union membership • physical or mental health details • religious or similar beliefs • sexual life For this type of information even more stringent measures should be employed to ensure that the data remains secure.

14 How this procedure will be implemented

Breaches of this policy will be investigated and treated as a disciplinary offence under the Trust's disciplinary procedure.

- This procedure will be published on the Trust's intranet and external website.
- Line managers will disseminate this procedure to all Trust employees through a line management briefing.

- This procedure will be reviewed every three years or more frequently if legislation or guidance from the Department of Health, the NHS Executive and/or the Information Commissioner changes.

14.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff	Induction training	1 day	Once
All staff	Network and NHSmail e-learning	As required to complete modules	Once

15 How the implementation of this procedure will be monitored

Auditable Standard/Key Performance Indicators		Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	Routine audit and monitoring of compliance	Managers	Ongoing as part of normal operational management responsibilities
2	Spot checks of compliance and understanding of Data Protection, information confidentiality and security policies and procedures	Continuous programme of audit and spot checks by Information Governance staff	Digital Safety and Information Governance Board

Audits will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the use, transfer and storage of information, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

16 Document control

Date of approval:	06 June 2018	
Next review date:	06 December 2021	
This document replaces:	CORP-0025-v6(1) Safe Haven Policy	
Lead:	Name	Title
	Andrea Shotton	Information Risk, Policy and Records Standards Manager
Members of working party:	Name	Title
	GDPR steering group	
This document has been agreed and accepted by: (Director)	Name	Title
	Patrick McGahon	Director of Finance and Information
This document was approved by:	Name of committee/group	Date
	Digital Safety and Information Governance Board	06 June 2018
An equality analysis was completed on this document on:	05 June 2018	

Change record

Version	Date	Amendment details	Status
1		Renumbered from CORP-0025 and revised from policy to a procedure Revised in line with Data Protection Act 2018 (GDPR)	Published
1	12 April 2021	Review date extended to 06 December 2021	Published

Appendix 1 - Equality Analysis Screening Form

Please note; The Equality Analysis Policy and Equality Analysis Guidance can be found on InTouch on the policies page

Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc.	Information Department					
Name of responsible person and job title	Andrea Shotton – Information Risk, Policy and Records Standards Manager					
Name of working party, to include any other individuals, agencies or groups involved in this analysis	GDPR steering group					
Policy (document/service) name	CORP-0026-007-v1					
Is the area being assessed a…	Policy/Strategy		Service/Business plan		Project	
	Procedure/Guidance			X	Code of practice	
	Other – Please state					
Geographical area covered	Trust-wide					
Aims and objectives	• Maintain the privacy and confidentiality of personal information; • Ensure compliance with legal requirements, especially concerning sensitive information (e.g. people's medical condition); • Give confidence to Trust staff, other Trusts or other agencies that personal information is being sent to a location which ensures the security of data.					
Start date of Equality Analysis Screening	16 May 2018					
End date of Equality Analysis Screening	05 June 2018					

1. Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?

Following this policy gives confidence to Trust staff, other Trusts or other agencies that personal information is being sent to a location which ensures the security of data:

- At the point of receipt.
- Whilst held by the department.
- When transferring information to others, by whatever means.
- When archived.
- At the point of disposal.

2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?

Race (including Gypsy and Traveller)	No	**Disability** (includes physical, learning, mental health, sensory and medical disabilities)	No	**Gender** (Men, women and gender neutral etc.)	No
Gender reassignment (Transgender and gender identity)	No	**Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.)	No	**Age** (includes, young people, older people – people of all ages)	No
Religion or Belief (includes faith groups, atheism and philosophical belief's)	No	**Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave)	No	**Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners)	No

Yes – Please describe anticipated negative impact/s **No** – Please describe any positive impacts/s Adhering to this procedure will ensure that data subjects can have confidence in how the Trust handles their personal, sensitive and confidential information. The procedure describes adjustments to be made to ensure accessibility to safe haven faxes, thereby supporting staff with physical disabilities.

3. Have you considered other sources of information such as; legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.? **If 'No', why not?**	**Yes**	**X**	**No**	

Sources of Information may include: • Feedback from equality bodies, Care Quality Commission, Equality and Human Rights Commission, etc. • Investigation findings • Trust Strategic Direction • Data collection/analysis • National Guidance/Reports	• Staff grievances • Media • Community Consultation/Consultation Groups • Internal Consultation • Research • Other (Please state below)

4. Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Gender, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership
Yes – Please describe the engagement and involvement that has taken place
The original version of this procedure (formerly a policy) underwent Trust-wide consultation. Trust staff comprise all protected characteristics.

No – Please describe future plans that you may have to engage and involve people from different groups

5. As part of this equality analysis have any training needs/service needs been identified?					
No	Please describe the identified training needs/service needs below				
A training need has been identified for;					
Trust staff	No	Service users	No	Contractors or other outside agencies	No
Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so					
The completed EA has been signed off by: You the Policy owner/manager: Type name: Andrea Shotton					Date: 05 June 2018
Your reporting (line) manager: Type name: Lorraine Sellers					Date: 05 June 2018

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Are people involved in the development identified?	Yes	
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Training**		
	Have training needs been considered?	Yes	
	Are training needs included in the document?	Yes	
7.	**Implementation and monitoring**		

	Title of document being reviewed:	Yes/No/ Unsure	Comments
	Does the document identify how it will be implemented and monitored?	Yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?		
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
Signature:		Andrea Shotton	

Appendix 3 – Information security notice

By following some simple steps we can do a lot to ensure our own office is a safe haven. Please display this information security notice in your office where everyone can see it. It is a useful reminder of what we should all do to ensure the security and confidentiality of personal (patient and staff) and sensitive business information.

INFORMATION SECURITY NOTICE

PLEASE CHECK THE FOLLOWING WHEN YOU LEAVE YOUR OFFICE

FILING CABINETS ARE LOCKED

ALL WORK IN PROGRESS CONTAINING PERSONAL AND SENSITIVE BUSINESS INFORMATION IS LOCKED AWAY

THE KEY CUPBOARD IS LOCKED

YOUR MONITOR IS LOCKED WHEN NOT IN USE

ALL ROOMS ARE LOCKED OVERNIGHT AND WHEN UNATTENDED

Appendix 4 - Developing Safe Haven Procedures Questionnaire

Security of the Safe Haven Area					
No.	**Question**	**YES/NO**	**Corrective action**	**Action Date**	**Notes**
1	Is the area separated for the general public by two access controls when unmanned, e.g. two locked doors or a locked door and all personal information is locked away.				
2	Is the area protected by an alarm system out of hours?				If No advice should by sought from the Trusts Health, Safety & Security Manager
3	Is access to this area restricted to those who work in that area?				
4	If the area is a shared area are staff aware that minimum information should be out at any time and put away as soon as it is finished with. It must also not be left in view of unauthorised staff				Any shared areas must be reported as a weakness and review made to try and locate a secure location.
5	In the event that unauthorised personnel require access to the safe haven area are they accompanied at all times and all personal information removed from view?				
6	Are staff aware that the area must be locked if it is to be left unattended?				
7	Where keypad locks are in place are the codes changed on a regular basis, i.e. quarterly?				

8	Are all staff aware and fully trained of information handling, transferring, sharing and security requirements?				See training presentations on the Information Governance Intranet Page and Connecting for Health e-Learning module
Security of Manual Records					
9	Is information in what ever format restricted to those who need to know it to do their job?				**NB.** Being an NHS employee does not in itself qualify an individual as needing to know.
10	Has a clear desk policy been implemented?				This must be a control built into the safe haven procedures for the area
11	Are all files containing personal information held securely when not in use? E.g. in locked filing cabinets or drawers				See Records Management Policy Information and Minimum Security Measures and document the appropriate measures for you area
12	Is access to files containing personal information etc. restricted to staff that need them to legitimately do their job?				See Records Management Policy
13	Are Records filed in such a manner that they can be quickly located if required?				See Records Management Policy
14	Has a tracking / tracing system been implemented?				See Records Management Policy
15	Are records held securely within files? E.g. bound				See Records Management Policy
16	Is it ensured that all confidential information is not visible through or on the				See Records Management

	files cover?				Policy
17	When copies of records are transferred is a record of that transfer maintained, to whom, and why?				See Records Management Policy
Security of Computer Records					
18	Are monitors placed so that information displayed on them can not be overseen? E.g. through a window or in an open reception area				
19	Have processes been put in place to ensure that information is saver to a main server and not the local computer?				
20	Have all system users been issued with individual passwords to the systems they require, limiting them only the information they require to do their job				
21	Are staff aware of there responsibilities in respect of passwords and systems access				See acceptable use policy
22	Are all staff aware that they must lock their computer or log out when leaving it unattended?				
Encryption.					
23	Where electronic storage media are used e.g. laptops, USB flash memory sticks, messages on phones etc. has it been ensured that adequate encryption has been installed and is in use.				Ensure that the risk register is up to date and contains the asset numbers for all electronic storage items. For assistance contact the IT Service Desk on 01642 283949

Protective Markings					
24	Has the service/department implemented the use of protective markings?				Asset numbers assigned should appear on the risk register of the area.
Visual Control Boards					
25	Where visual control boards are in use have they been placed in areas that can be over seen by the public or unauthorised personnel?				
26	Is it policy to ensure that information recorded on white boards is anonymised?				
27	Is it policy to record only the minimum information required on white boards?				
Transferring Information					
28	Are Staff aware of both the NHS Code of Confidentiality and Caldicott principles.				
29	Have appropriate staff been authorised to transfer information?				
30	Are staff aware of situations where the data subjects consent is required before information can be transferred.				
31	Have secure methods of transfer appropriate to the information being transferred been determined and implemented?				
Staff taking information off Trust premises.					
32	Do staff needing to remove confidential information from Trust premises obtain the				

	appropriate approval to do so and is this approval recorded?				
33	Is a record made of information taken off site?				
34	Is it ensured that only the minimum required is transported?				
35	Are staff aware that they are bound be the same rules of confidentiality and must keep records safe and secure at all times whilst away from their place of work?				
36	Has a tracer system been implemented to record the removal of files?				
37	Have appropriate transportation methods been implemented? E.g. carried in a locked container case to ensure nothing is lost.				
38	Are staff aware that when records are to be transported and on occasions left in vehicles that they must be in the boot and in a locked container and must comply with the Records Management Policy. **NB/** Records must never be left in vehicles for long periods, e.g. over night				Should this be necessary it must be recorded and bought to the managers attention beforehand and must be locked in the **car boot**, in a locked container. Darkened windows do not suffice as a deterrent.
39	Are staff aware that records are not to be left in easily accessible areas in whatever format.				
40	Are staff aware that when records are taken home care must be taken to ensure they are suitably secured and not				

	accessible to other members of the household or visitors?				
41	Is it ensured that records are returned to Trust premises as soon as possible?				
Identifying Information Flows					
42	Does your department send routine reports or bulk amounts of information to other departments or organisations?				
43	Have these information flows been mapped?				To check, contact the IG Team on 0191 333 6574
44	Have appropriate controls been implemented to protect this information in transit?				
Mail – Incoming					
45	Are staff aware letters marked safe haven must not be opened by other than an authorised member of staff?				
46	Is correspondence containing personal or sensitive material locked away when the safe haven in unattended?				
47	Are staff aware any safe haven correspondence received in error must be resealed and forwarded immediately to the correct recipient or if not know returned to sender. Ensuring the packaging is marked **Safe Haven, Private and Confidential**				
Mail – Outgoing					
48	Are staff aware that all outgoing letters are marked **private and confidential –safe**				

	haven addressee only?				
49	Are Staff aware of the correct packaging methodologies for confidential information being sent out?				
50	Are Staff aware of the correct method for sending confidential information being sent out, e.g. courier, post or by hand?				
51	Is all outgoing mail marked **Private and Confidential to be opened by addressee only. Are staff aware that the envelope should contain a return address in case of misdirection?**				
Couriers					
52	Does your service use couriers where it has been determined that the postal system is not sufficiently secure?				
Fax					
53	Is the fax machine situated in a secure area and access to it is only available to authorised staff.				
54	The fax is a dedicated safe haven only fax and used only for safe haven purposes.				
Incoming Faxes					
55	Are incoming faxes collected regularly by authorised staff.				
56	Is it standard practice to store incoming faxes in the fax machine buffer out of hours ready for printing by an authorised member of staff?				

57	Are staff aware that faxes containing personal information incorrectly received must be placed in a sealed envelope, marked appropriately as per mail above and forwarded to the addressee of the fax?				
Outgoing Faxes					
58	Are key Safe Haven faxes numbers pre-programmed into the machine to avoid misdialling?				
59	Do staff know to double check individually keyed numbers before sending?				
60	Do staff make the recipient aware of the transmission of a fax when sending to a none pre-programmed number requesting acknowledgement of receipt?				
61	Are faxes marked **PRIVATE AND CONFIDENTIAL** and is the address checked prior to sending?				
62	Are staff aware to use the minimum patient details possible e.g. using NHS Number or Paris ID in place of the patients name?				
Email – Incoming.					
63	Do staff remove emails containing personal information from their email system and file securely as soon as possible.				**NB**, personal information should not be held on email system longer than absolutely necessary.
Email – Outgoing					
64	Do staff consider whether email is the most				

	appropriate method to send the information – can another method be used? **NB/** emails can easily be forwarded to others against your wishes.				
65	Are recipients of the email kept to a minimum and are these recipients checked to ensure they are the correct ones before the email is sent.				This can be done be checking the properties of the recipients address – call the IT Service Desk on 01642 283 949
66	Are Staff aware the any emails containing personal information must be sent from and to an NHS Mail (or other secure) account?				
67	Do staff ensure that the minimum information is sent for the recipient to be able to carry out their job?				
68	Are staff aware that they must never use personal identifiable information in the subject line?				
69	Do staff mark the emails **CONFIDENTIAL?**				
70	Is a disclaimer placed on the email stating that the recipient is responsible for the security and confidentiality of the data within that email and that data must not be passed on to others via any method unless they have a justified need to know?				
Telephones Conversations					
71	Are all staff aware that any conversations regarding personal or confidential information must take place in a safe				

	haven area or other place where they can not be over heard?				
72	When speaking to service users or careers do staff confirm the callers' identity or call back?				
73	Are staff aware to use the secrecy button when putting callers on hold?				
74	In the event of requests for information by telephone do staff confirm the identity of the requestor and their authorisation to receive the information. This could mean calling the enquirer back via a main switch board **DO NOT** use direct lines for this verification purpose				
Answer Phones – Incoming					
75	When checking messages on an answer phone ensure they can not be overheard by unauthorised personnel?				
76	If message books are used is it ensured that these are held securely?				
Answer Phones – Outgoing					
77	Are staff aware that in the event that they have to leave an answer phone message that they only request the contactee to call back leaving a name and phone number?				
Verbally transfer of information					
78	Are staff aware that whenever they are transferring information verbally, either formally or informally that they must ensure				

	they are not overheard. Where possible do not identify the service user?				
79	Where service users registering at reception is it ensured that any personal details they need to give can not be overheard.?				
80	Where discussions must take place in a community area e.g. shared office or ward are staff aware that they are expected to respect patients rights?				
81	Where message books are used is it ensured that these are held securely?				
Information Sharing					
82	Are staff aware of their responsibilities in respect of information sharing?				
83	Are staff aware of guidance available i.e. the NHS Code of Confidentiality?				The NHS Code of Confidentiality is available on the Information Governance Intranet Page IG Policies and Guidelines
84	Has responsibility for making Information sharing decisions been delegated?				
85	Where information is shared with other agencies has an Information Sharing Protocol been put in place?				
Subject Access Requests					
86	Have staff been made aware for their responsibilities in respect of patients requesting copies of medical records?				The Data Protection Act Subject Access Request form, and associated written

87	Are staff able to advise service users on how to apply for a copy of their records.				procedures and processes are available on the trust intranet IG pages under the Data Protection Section. Further advice can be obtained from the Data Protection Officer on 0191 333 6213
88	Are all records reviewed by an appropriate clinician to ensure no exempt information is sent out? E.g. third party information				
Out of Hours					
89	Have Out of Hours situations been reviewed to ensure that adequate security has been implemented for all of the above.				
Disposal of Information					
90	Have the correct methods of disposing of information securely and confidentiality whatever its format have been identified and implemented?				
Reporting Incidents					
91	Are staff aware that all breaches of information or safe haven area security or confidentiality must be reported, including near misses?				
Highlighting Security weaknesses					
92	Are staff aware that they are responsible for reporting security weaknesses to their manager for corrective action?				
Documented Procedures					
93	Have the controls identified in completing this questionnaire been documented and				

	communicated to staff?				
Training					
94	Have staff been trained in these procedures? Are new starters made aware of this on local induction?				