NHS 24

Data Protection Audit Report

V1.0

Auditors:	Christine Eckersley	Engagement Lead Auditor
	Claire Chadwick	Lead Auditor
	David Simmons	Lead Auditor

Distribution:

Draft Report: Dr Malcolm Alexander, Associate Medical Director, Alison Morton, Information Governance Manager, Sanny Gibson, Information Security Manager

Final Report: John Turner Chief Executive, George Crooks Medical Director, Dr Malcolm Alexander – Associate Medical Director

Date Issued: 2 December 2010

Contents

1. Background

1.1 In January 2010, following a Privacy Impact Assessment presentation to the NHS Scotland Information Governance Network, ICO Scotland were approached by a representative of the Information Governance team at NHS 24.

1.2 NHS 24 requested that the ICO conduct an audit, in order to help them assess levels of compliance with the requirements of the Data Protection Act (DPA) and with good Information Governance practice and to raise awareness of these issues.

1.3 The ICO Audit Group agreed to conduct an audit for the purpose of identifying and promoting data protection good practice within NHS 24, to enable them to build upon initiatives already implemented in this area. This audit was at the request of NHS 24 and was not the result of a data protection breach.

1.4 Following further discussion between NHS 24 and the ICO Audit Group, regarding audit scope and availability of staff, arrangements were agreed for the audit to take place at NHS 24 Headquarters, Cardonald and the NHS 24 Contact Centre, Clydebank.

1.5 The Audit was undertaken from the 24th to 26th August 2010.

2. Audit Opinion

Overall Conclusion	
Limited Assurance (Medium priority)	On the basis of the work performed at NHS 24 we consider that the current arrangements in place, with regard to overall Data Protection controls provide a limited assurance that adequate processes and procedures are in place and being adhered to. NHS 24 proactively volunteered to participate in a 'consensual' audit to assist it in identifying good practice, to identify levels of compliance and to further raise levels of awareness of data protection concerns within the Board. The level of assurance for Data protection Governance has been assessed as reasonable (low priority) two further reasonable assurance assessments have been provided for the processing of patient information and the processing by Human Resources of employee personal information. Examples of good practice identified in these areas are detailed below. Three medium priority assessments have been made for Information Security, Training and awareness and Information security incident reporting. The key findings are summarised below. The ICO recommendations focused on these areas are provided to improve the arrangements currently in place.

3. Summary of Audit Findings

Areas of Good Practice

In response to a combination of external audits, internal feedback and some new KPI reporting processes, NHS 24 is planning recommended improvements to some areas of IT and information security provision, Information Governance and Risk training provision.

Call handlers and nurse practitioners described regular checks/quality assurance of their work, to assess procedural compliance and quality.

NHS 24 employs 'ethical hackers' every 12 to 24 months to carry out penetration attacks on the network and assess system security.

Staff interviewed during the audit were aware that the IG policies were available on the intranet and also knew to contact the Information Governance Manager and Information Security Manager directly for advice.

Laptop builds have been configured to ensure no user data is saved to local portable drives but is instead saved to the main NHS 24 server. In this way NHS 24 is complying with the E-Health instructions and personal data is appropriately secured.

NHS 24 is building privacy impact assessments into its systems and processes and has participated in an ICO run workshop to inform this activity.

Areas for Improvement

Responsibility for the security of NHS 24 buildings should be clearly assigned.

Policies should be reviewed and updated in line with NHS 24 document review dates to ensure currency of advice and content.

Data protection training and refresher provision should be introduced as planned, for all staff, including those at senior manager or executive level.

Information security incidents involving personal data should be included on KPI's or other Management Information, to measure and address issues of non compliance.

Both the Information Governance Manager and the Information Security Manager should be formally informed about the nature of data sharing agreements, to assess DPA and Information Security considerations.

NHS 24 should ensure that password requirement is sufficiently 'strong' for purpose.

At present NHS 24 do not provide specific data security training, which is key to ensuring staff understanding of the security of patient and staff personal data.

Staff have optional 'secure printing' of documents, from the printer queue following the input of their user password. However, 'secure printing' is not routinely used. This is a potential security risk for printed documents containing personal data, within the NHS 24 open plan working environment.

HR Files should be appropriately weeded before archiving to ensure archived information is not excessive or being kept for longer than necessary, in line with NHS 24's data protection responsibilities

4. Audit Approach

4.1 The audit was carried out in accordance with the Information Commissioner's data protection audit methodology, comprising a desk-based review of submitted policies and procedures, and an on-site visit including interviews with selected staff.

4.2 The audit field work was undertaken at the NHS 24 Headquarters Cardonald Park, Glasgow and NHS 24 Contact Centre, Golden Jubilee National Hospital, Clydebank from 24 to the 26 August 2010. This involved interviews with a wide selection of staff from senior managers to call handlers and discussion and observation of relevant procedures and processes.

4.3 Due to NHS 24 sensitivity regarding Auditor access to confidential patient records, it was not possible to examine the processing of incoming information against input to database records. However, Auditors were given guided access to the training database for familiarisation with relevant input fields and a number of interviews were undertaken with both call handlers and nurse practitioners regarding procedures for the receipt and processing of information.

5. Scope of the Audit

A wide audit scope was requested. This included:

a. Information Governance – to include organisational structure, roles, responsibilities, reporting, policy and procedures and risk management functions in respect of data protection issues.

b. Information Security - The processes in place to ensure appropriate technical and organisational measures are applied for the security of manual and/or electronic patient personal data.

c. The provision of staff training and awareness in relation to data protection issues.

d. The processes for the identification and reporting of data protection security breaches.

e. Clinical Records – Data handling in respect of all clinical records i.e. the receipt, processing, storage and weeding of patient personal data.

f. Staff data – Data handling in respect of all staff records, i.e. the receipt, processing, storage and weeding of staff personal data.

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 definitions in the table below.

Colour Code	Audit Opinion	Recommendation Priority	Definitions
🟩	Good assurance	**Minor points only are likely to be raised**	The arrangements for data protection compliance with regard to governance and controls provide a high level of assurance that processes and procedures are in place and being adhered to and that the objective of data protection compliance will be achieved. No significant improvements are required.
🟨	Reasonable assurance	**Low priority**	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed to enhance the likelihood that the objective of data protection compliance will be achieved.
🟧	Limited assurance	**Medium priority**	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The achievement of the objective of data protection compliance is therefore threatened.
🟥	Very Limited assurance	**High priority**	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore 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

Findings flowing from the audit will be risk categorised using the criteria defined in Section 6. The rating will take into account the impact of the risk and the probability that the risk will occur.

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.1 Information Governance – to include organisational structure, roles, responsibilities, reporting, policy and procedures and risk management functions in respect of data protection issues.				
a.	To examine if there is a failure to identify and implement a system whereby data protection governance can be managed, measured and reported, raises the risk of the organisation having no visibility of how it is meeting its obligations, resulting in data protection issues not being identified and addressed.	7.1.1The NHS 24 Medical Director is also the Caldicott Guardian and is the named NHS 24 Board member with overall Information Governance (IG) responsibility. 7.1.2 The Caldicott Guardian is the 'Executive Sponsor' of the Information Governance Steering Group (IGSG) and is represented by the Associate Medical Director at IGSG meetings. 7.1.3 The Information Governance Manager and the Information Security Manager are also members of the IGSG. Auditors were advised by the Senior Information Risk Officer		No action required No action required No action required

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
🟨		(SIRO) that he is represented on the group by the Information Security Manager.		
		7.1.4 The Head of Risk & Business Continuity is based in the Medical directorate and is responsible for devising and implementing relevant risk strategies in NHS 24. He has formal links with the Information Security Manager, who is a Deputy Risk Lead.		No action required
		7.1.5 There appears to be no formal mechanism for the Caldicott Guardian or Senior Executives to inform the Information Governance Manager, or Information Security Manager, about potential or approved NHS 24 data sharing agreements. This raises the risk that data sharing agreements may not always be assessed for compliance against relevant Data Protection legislation.	7.1.5 Both the Information Governance Manager and the Information Security Manager should be included in or informed about the nature of data sharing agreements, to assess compliance with the legal requirements of the Data Protection Act.	7.1.5(i) A new standing item to be added to the IGSG – Data Sharing Agreements. The Caldicott Guardian and SIRO will routinely be asked for details of any new data sharing agreements for review at the group. ***Action: AMD****.* ***By: Nov10***

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
🟨		The auditors were informed however that the IG Manager is made aware of and has the opportunity to challenge all instances of data sharing prior to sending of information, through controls applied by the information services team.		7.1.5.(ii) PIAs will continue to be rolled out across the organisation No action required
		7.1.6 Information Governance KPI's are provided to the Executive Team. The IG Manager assesses timescales / toolkit progression and compliance with the SAR 40 day deadline for DPA compliance. The IG Manager is also responsible for overseeing information access requests, policy, PIA issues, records management (including patient), & IG toolkit co-ordination		7.1.6. No action required
		7.1.7 The Information Governance Manager ensures smooth running of and provides an administration function to the Information Governance Steering Group, which reports by exception into		7.1.7. No action required

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
🟨		the National Clinical Governance Group and (via the Clinical Governance Committee,) the NHS 24 Board.		
		7.1.8 The IG Manager introduced Information Governance policy and procedures and deals with other DP issues including the FOISA publication scheme. However, there is no specific Data Protection policy and a number of documents reviewed (for example the IG Policy statement,) have not been updated for some years. A policy review exercise is currently being undertaken which should assist in the process.	7.1.8 Policies should be updated as soon as possible and ongoing reviews should be undertaken, in line with NHS 24 document review dates.	7.1.8(i) A schedule of policy review will be put in place and monitored by the IGSG. ***Action: AMD/IGM*** ***By: Nov 10*** 7.1.8.(ii) The Process Team will manage the policy review schedule on behalf of the IG and IS Managers ***Action: ISM/IGM*** ***By: Dec 10*** 7.1.8.(iii) Develop draft Data Protection Policy ***Action: IGM*** ***By: Nov 10***

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
🟨		7.1.9 There are no Data Protection representatives or staff forums, below management level for discussion, dissemination or raising awareness of Data Protection issues within NHS 24.	7.1.9 Data protection ‘representatives’ at team or directorate level may be useful for the local discussion and reporting of DP issues and may assist the IG Manager in disseminating DP issues.	7.1.9.(i) Refresh face to face training and awareness for all staff including senior management. ***Action: ISM/IGM*** ***By: Feb 11*** 7.1.9(ii) Develop communication plan re awareness of Data Protection. ***Action: ISM/IGM/Head of Internal Comms*** ***By: Feb 11*** 7.1.9(iii) Regional Governance Groups to add Information Governance and Security standing item on their agendas ***Action: ADONs*** ***By: Jan 11***

<table>
<tr><th>Ref</th><th>Compliance Risk</th><th>Issues / Findings</th><th>Recommended Solution</th><th>Management Comments, Responsibility for Action and Due Date</th></tr>
<tr><td>🟨</td><td></td><td>7.1.10 Risks containing an ‘Information Governance’ tab are transferred from the risk register to a separate IG risk register, which is ‘owned’ by the IG Manager. The risks are reviewed as part the IGSG meetings.</td><td></td><td>No action required.</td></tr>
<tr><td colspan="5"><b>7.2 Information Security - The processes in place to ensure appropriate technical and organisational measures are applied for the security of manual and/or electronic patient personal data.</b></td></tr>
<tr><td rowspan="3">🟧 b.</td><td rowspan="3">To examine if there is a failure to implement measures which adequately protect manual and electronically held personal data raises the risk of inappropriate access to, damage to, destruction or loss of data, leading to potential damage and distress being caused to the affected individuals and reputational damage to the Board</td><td>7.2.1 The Head of Technology is responsible for NHS 24 networks, applications and hardware, new projects including defining requirements, programme management and supply management.</td><td></td><td>No action required</td></tr>
<tr><td>7.2.2 The Information security Manager is based in the Finance & Technology Directorate, reporting to the Technology Quality and Test Manager.</td><td></td><td>No action required</td></tr>
<tr><td>7.2.3 The IS Manager role covers both physical and ICT security advice, input to the</td><td></td><td>No action required</td></tr>
</table>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
🟧		risk register, reviewing training provision and e-learning packages and the management of the Information Security Management System. Policies and procedures have been written to comply with the ISMS related ISO27001 standard which has been subject to internal review, but not yet a formal ISO assessment.		
		7.2.4 It was reported that there is no clear responsibility for physical security within NHS24 sites. This lack of clarity is in itself a security risk, due to the associated lack of accountability.	7.2.4 Responsibility for the security of NHS 24 buildings should be clearly assigned. As this relates to physical security of patient records and computer assets, it may be good practice to include this within the remit of Information Security	7.2.4. Review ISM job description to expand, clarify, formalise and document the physical security aspects to ensure clarity of responsibility. ***Action: ISM*** ***By: Mar 11***
		7.2.5 There is no procedure to cover disabling of lost security badges and no formal procedure to cover issuing and tracking of temporary passes.	7.2.5 A formal procedure should be introduced for the disabling and tracking of building security passes.	7.2.5. Formalise procedure on completion of badge access system. ***Action: ISM*** ***By: Dec 10***

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
🟧		7.2.6 NHS24 operates its own dedicated network and domain (nhs24.net) covering all offices plus remote access to approx. 50 flexible workers. Flexible workers use VPN dual authentication access control. Remote users have limited access to their own shared drives and email only.		7.2.6(i) Refresh physical security and ID badge policies to ensure that they specify that all visitors require an NHS 24 host whose responsibilities include badge return at end of each visit. ***Action: ISM/Head of Internal Comms*** ***By: Jan 11*** 7.2.6.(ii) Introduce Visitor Management software module with associated reception area badge readers on the badge access system to introduce further controls in this area. ***Action: ISM*** ***By: Mar 11***
		7.2.7 PCs are used by office staff and the use of the C: drive is disabled. Data is stored in server drives and departmental folders. Sound		7.2.7. No action required

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		cards and CD drive write function is also disabled.		
		7.2.8 There are some weaknesses with ‘total view’ passwords regarding length option and expiry times, which raises access security risks.	7.2.8 As access control is dependent on password rather than smartcards or equivalent, NHS 24 should ensure that password requirement is sufficiently ‘strong’ for purpose.	7.2.8(i) Review password policy and update password complexity requirements to provide enhanced protection and ensure password requirement sufficiently strong for purpose. ***Action: ISM/Head of Internal Comms*** ***By: Jan 11*** 7.2.8.(ii) Investigate and implement alternative solution to nationally funded Identity Access Manager System ***Action: ISM*** ***By: Jun 11***
		7.2.9 Secure printing is available via password protected queues but this is not the default and is a potential security risk for open plan working.	7.2.9 Where available, Secure printing should be the default setting to ensure the security of, and appropriate access to, patient data.	7.2.9. Define Safecom pull print solution as the default print solution for NHS 24. ***Action: ISM***

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		7.2.10 NHS 24 now use KPMG as internal IT auditors as well as Audit Scotland, and the current event logging system has been recognised as an area for improvement 7.2.11 In Learning & development, and recruitment, keys to cupboards containing confidential paper files are kept in a desk drawer or taken home by a member of staff.	7.2.10 The event logging system deficiencies should be mitigated by the reported NHS 24 planned purchase of a more efficient system. 7.2.11 Provision should be made for keys to confidential L&D and Recruitment files to be stored securely and to be appropriately accessible where required.	***By: Feb 11*** 7.2.10 Source a set of logging tools to address deficiencies. ***Action: ISM*** ***By: Mar 11*** 7.2.11. **Complete**
7.3 The provision of staff training and awareness in relation to data protection issues.				
c.	To examine if there is any failure to implement measures which adequately ensure appropriate staff training and awareness of Data Protection issues raises the risk of inappropriate access to, damage to, destruction or loss of data, leading to	7.3.1 The Caldicott Guardian received a half day training course 5 years ago and has received no refresher training since undertaking the role. The Senior Information Risk Owner (SIRO) has received no formal training for his role. 7.3.2 The Information Governance department carried out classroom based data	7.3.2 Data protection training and refresher provision should be	7.3.1. Identify and procure formal Caldicott Guardian/SIRO training. ***Action: Head of L&D/ISM*** ***By: Mar 11*** 7.3.2. Relaunch updated IG & IS training

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
🟧	potential damage and distress being caused to the affected individuals and reputational damage to the Board	protection training until about 18 months ago when it was suspended due to the swine flu epidemic. However, there are plans to reintroduce the training, which will be mandatory and subject to compulsory refresher sessions, every two years.	introduced as planned, for all staff, including those at senior manager or executive level.	***Action: ISM/IGM*** ***By: Mar 11***
		7.3.3 Staff currently complete the IG e-learning training which is mandatory. Once the e-learning is complete it is logged electronically and reports can be produced showing who has completed the course.		7.3.3. No action required
		7.3.4 Auditors assessed the IG training content. This covers various aspects of IG including the DPA. The training covers principle 1 & 6 effectively, relating them to the NHS 24 environment and gives practical examples on how these principles should be complied with at NHS 24.		7.3.4. No action required

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
🟧		7.3.5 Principles 3, 4 & 5 are not dealt with in sufficient depth.	7.3.5 Principles 3 (adequacy and relevance), 4 (accuracy) and 5 (retention) should be more fully included in data protection e-learning to ensure staff awareness.	7.3.5. Rewrite elearning module to ensure all principles are covered. ***Action: ISM/IGM*** ***By: Feb 11***
		7.3.6 Principle 7 is to be covered in other training, but at present there is no training on data security.	7.3.6 Data security training should be provided, to ensure staff awareness and support compliance with NHS 24 data protection responsibilities.	7.3.6. Relaunch data security training to ensure staff awareness. ***Action: ISM/IGM*** ***By: Feb 11***
		7.3.7 Auditors accessed the staff intranet to assess the availability of policies and procedures. The Intranet is not user friendly and has a poor search facility, which did not always retrieve related items.	7.3.7 Improvements should be made to the search facility to assist staff in retrieving appropriate guidance.	7.3.7. Ensure redesign of intranet provides search facility fit for purpose. ***Action: Head of Internal Comms*** ***By: Mar 11***
		7.3.8 Guidance is not easily located, for example IT related policies were accessed via the 'HR' link and all IG related policies were accessed under the 'Medical' link.	7.3.8 Placing guidance under a central heading , rather than by Directorate, may assist staff in locating relevant IT and IG policies	7.3.8. Develop link to all policies from front page of intranet ***Action: Head of Internal Comms/ISM/IGM*** ***By: Dec 10***

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
🟧		7.3.9 The ‘data protection’ intranet link is empty. The IG policy statement provided to audit includes some basic guidance on DP principles, but auditors could not locate this document on the intranet.	7.3.9 NHS 24 to ensure that staff have full access to data protection information to ensure staff compliance with Data Protection legislation	7.3.9. Populate DP link on intranet with basic DP guidance. ***Action: IGM*** ***By: Dec 10***
		7.3.10 A short term project is currently under way to review NHS 24 policies, fitness for purpose and staff awareness of them	7.3.10 Findings from the project should be used to improve NHS 24 provision and staff awareness of policies.	7.3.10(i). Develop audit plan following outcome of project. ***Action: ISM*** ***By: Dec 10*** 7.3.10(ii) Implement Metacompliance to ensure staff awareness ***Action: ISM*** ***By: Mar 11***
		7.3.11 A number of interviews were undertaken with NHS 24 staff regarding Data Protection training. All staff interviewed had completed either the IG e-learning or classroom training at least once, although in some cases this was a number of	7.3.11 Refresher training for staff should be provided to support compliance with relevant DP legislation.	7.3.11. Annual e-learning module to be completed for all staff ***Action: Head of L&D*** ***By: Feb 11***

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		years ago. Not all staff could recall the content of the training. 7.3.12 All staff interviewed were aware that the IG policies and procedures were available on the intranet. However, In the case of specific queries staff would either consult the IG Manager or the Information Security Manager for Advice.		7.3.12 No action required

7.4 The processes for the identification and reporting of data protection security breaches.

d.	To examine if there is any failure to implement measures for the identification and reporting of data security breaches raises the risk of the organisation failing to identify, mitigate or prevent further security breaches leading to potential damage and distress being caused to the affected individuals and reputational damage to	7.4.1 The Information Security manager is responsible for investigating all incidents involving personal data in addition to other IS incidents. 'Incidents' cover IT, manual and spoken information security breaches. The incident reporting policy is available to staff on the intranet.	.	7.4.1. No action required

🟧	NHS 24.	7.4.2 Auditors reviewed the NHS 24 Staff Information Security Policy (Incident/Risk reporting) and NHS 24 Security Incident Management Policy. The definition of incident on either policy does not clearly include the loss or compromise of personal data.	7.4.2 Loss/compromise of personal data should be included within incident reporting and managing policies to appropriately instruct staff.	7.4.2. Add to relevant policies during the IS policy review. ***Action: ISM/Head of Internal Comms*** ***By: Mar 11***
		7.4.3 The policy States that the IS Manager will carry out an annual audit of compliance although no evidence was provided to support this.	7.4.3 The IS manager should ensure the annual audit is completed to ensure compliance with incident and risk reporting process.	7.4.3. Complete annual audit to ensure compliance with incident and risk reporting process. ***Action: ISM*** ***By: Jun 11***
		7.4.4 The process for escalating risk incidents to the IS Manager may be inadequate. Front line staff use the 'AIR' reporting system which does not specifically define loss/compromise of personal data as an incident.	7.4.4 The Information Security Manager should ensure staff awareness of reporting requirements for information security incidents.	7.4.4. Roll out policies via Metacompliance ***Action: ISM*** ***By: Mar 11***

🟧		7.4.5 Only one incident has been reported to the IS Manager in 3 months. This was supported by interviews with call handlers and nurse practitioners which indicated a lack of knowledge and consistency in reporting incidents.		7.4.5. No action required
		7.4.6 The Head of Risk and Business Continuity devises and delivers risk training via the L&D department. However, he has received recent feedback from staff concerning a lack of understanding on the risk scoring system.	7.4.6 Risk Training should be amended, as planned, to address this knowledge gap and support appropriate recognition and mitigation of identified risk levels.	7.4.6. **Complete**
		7.4.7 IS incidents are not a current KPI. Other than manually counting incidents it is not possible to produce MI on incidents involving only personal data. This means that there is no evidence being presented to board level showing possible non compliance with the DPA	7.4.7 Information security incidents involving personal data should be included on KPI's or other Management Information, to measure and address issues of non compliance.	7.4.7. Develop KPI for reported incidents ***Action: ISM*** ***By: Nov 10***

🟧		7.4.8 The AIR system is mainly used by frontline staff (Call handlers/nurse practitioners etc) Guidance is available on how to complete the form on the Knowledge Management System, which is not generally used by NHS 24 support staff	7.4.8 Guidance on the use of incident reporting systems should be widely available to all staff to ensure appropriate reporting of incidents.	7.4.8. Develop and disseminate incident reporting guidance for staff ***Action: ISM/Head of Internal Comms*** ***By: Mar 11***
		7.4.9 The Current corporate objective of an improved electronic risk system has not been implemented as hardware / software, re-bid is currently pending.	7.4.9 The implementation of the new electronic risk system may assist in improving risk reporting, in particular if there is a provision for risk likelihood to be reported by staff as well as incidents.	7.4.9. This is part of the Strategic Frontline Application project and will be an ongoing process. ***Action: Head of Implementation - SFLA*** ***By: ongoing***
7.5 Clinical Records – Data handling in respect of all clinical records i.e. the receipt, processing, storage and weeding of patient personal data.				
e.	To examine if there is any failure to appropriately receive, store, process and weed patient personal data raises the risk of inappropriate access to damage to, destruction or loss of patient personal data, contrary to the rights of patients and requirements of the Data Protection Act.	7.5.1 Incoming information is received via phone calls from members of the public. The majority of calls involve giving name, address, DOB and telephone number at the location.		7.5.1. No action required
		7.5.2 The PRM system sends information on each patient contact to the GP via an interface to the GP out-of-		7.5.2. No action required

		hours system known as ADASTRA. The ADASTRA system only accepts information and cannot interrogate PRM.		
		7.5.3 The call handler checks incoming patient details against a version of the 'CHI' database, for accuracy and security. The national CHI database (Community Health Index) contains patient GP details including name, DOB, address held at GP surgery. No medical details are accessible		7.5.3. No action required
		7.5.4 Call handlers/nurse practitioners also have access to ECS (Electronic Care System) which records patient medications and allergies. Some patients may also have a PCS record (Palliative Care Summary) which includes medicines, and other care requirements.		7.5.4. No action required
		7.5.5 Some trained call handlers perform a limited 'triage' (assessment) of symptoms based on a drop down menu of symptoms, prior		7.5.5. No action required

🟨		to transferring the call to an advisor, where appropriate.		
		7.5.6 Nurse advisors ask further clinical questions resulting in an 'outcome' i.e. referral to GP, ambulance, A&E, etc. The Adviser completes a clinical summary and narrative account on the patient's PRM record. The PRM system records the patient medical history and archived medical history.		7.5.6. No action required
		7.5.7 Patients are always asked for consent concerning transfer of information (i.e. to A&E, Out Of Hours Service, etc). If no consent is given, patients are informed of the possible consequences. A warning of 'data transfer consent not given' appears if the no consent' box is ticked and a transfer is attempted.		7.5.7. No action required
		7.5.8 Incoming information is stored on the electronic voice recording system or on the NHS 24 PRM system. It was reported that no paper patient files are used or kept by call		7.5.8. No action required

		handlers or nurse practitioners.		
		7.5.9 NHS 24 uses 'electronic faxing' for external services A standard format record of the call, symptoms; etc is forwarded to known contact numbers on the electronic system.		7.5.9. No action required
		7.5.10 Information sharing may occur with the police, social services, etc, by Nurse Advisors. Where outside agencies are involved, the matter is sometimes discussed with the Team Leader. Confidentiality / need to know is always a priority, in line with Caldicott principles and NHS 24 also provide procedural guidance on this.		
		7.5.11 In cases of computer 'System Malfunction' call adviser notes from incoming calls have to be taken manually and are later 'repatriated' with the computer record. When the system is restored the Team Leader allocates call handlers documents to 'repatriate' (input) into the system.	7.5.11 PRM records should be routinely checked against a sample of repatriation documents to confirm accuracy of transcription.	7.5.11. Develop a method for auditing the accuracy of transcription of repatriated records ***Action: ADONs*** ***By: Feb 11***

🟨		However, it was reported that input of the repatriated documents is not checked for accuracy.		
		7.5.12 Repatriated records are held securely prior to archive with an authorised document storage company.		7.5.12 No action required
		7.5.13 Call handlers and nurse practitioners were unaware of document retention periods; however, they are not responsible for any weeding or deletion of IT system information.		7.5.13 No action required
		7.5.14 It was reported that the document retention policy is relatively new within the organisation and plans are in place to take this forward with front line representatives being integral to the process.		7.5.14 No action required
		7.5.15 Call handlers and nurse practitioners consistently described routine checks/quality assurance on their work. There is a monthly one to one with the team leader or senior call handler who listens to recorded		7.5.15 No action required

		calls for QA purposes. A written record is kept of the monthly review and signed off by call handler.		
7.6 Staff data – Data handling in respect of all staff records, i.e. the receipt, processing, storage and weeding of staff personal data.				
f.	To examine if there is any failure to appropriately receive, store, process and weed staff personal data raises the risk of loss, inappropriate access to, retention of, or destruction of staff personal data, contrary to the rights of individuals and requirements of the Data Protection Act.	7.6.1 NHS 24 Main staff files are paper based and kept in lockable cupboards by HR in Cardonald HQ. 7.6.2 Electronic records are stored on the CIPHR database. HR also access payroll data to reconcile against entries on the CIPHR database. 7.6.3 NHS24 is starting the migration to the new Scottish Workforce Information Standard System (SWISS) for HR and this will eventually replace CIPHR. 7.6.4 CIPHR data sets are sent to SWISS and HR system support staff can access NHS24 staff details on SWISS as well as use the data to generate MIS reports. 7.6.5 Any files requested by third parties such as HR		7.6.1. No action required 7.6.2. No action required 7.6.3. No action required 7.6.4. No action required 7.6.5. No action required

🟨		partners in regional offices will be couriered and tracked. However, if only part of the file is relevant, pages are scanned and emailed using the secure NHS.net, where available. Files will always be sent to regional HR Partners by default, rather than to a requesting line manager.		
		7.6.6 Nominated HR staff are responsible for ensuring all cupboards are locked at end of day and keys are secured in key-pad key safe.		7.6.6. No action required
		7.6.7 HQ based HR staff have the use of secure Safecom printing option for three main printers on their open plan floor, however, this option has to be actively selected, and is not the default setting.	7.6.7 Where available, Secure printing should be the default setting to ensure the security of, and appropriate access to, staff data.	7.6.7. Define Safecom pull print solution as the default print solution for NHS 24. ***Action: ISM*** ***By: Feb 11***
		7.6.8 Old files are sent to archive run by commercial specialist, Iron Mountain but are not weeded before being sent out. HR manager is aware of need to review this.	7.6.8 Files should be appropriately weeded before archiving to ensure archived information is not excessive or being kept for longer than necessary.	7.6.8. Develop procedure for weeding information prior to archive. ***Action: Head of HR Shared Services*** ***By: Dec 10***

🟨		7.6.9 Staff interviewed had limited awareness of retention policies for files.	7.6.9 Staff should be made aware of the need to weed documents in line with NHS 24 retention policies, where appropriate.	7.6.9. Develop HR procedures for records management. ***Action: Head of HR Shared Services*** ***By: Dec 10***