Police Service of Scotland

Data protection audit report (2)

Information Commissioner's Office

Auditors: [redacted]

Data controller contacts: [redacted]

[redacted]

[redacted]

Distribution:

Date of first draft:	14 October 2016
Date of second draft:	4 November 2016
Date of final draft:	2 December 2016
Date issued:	**2 December 2016**

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 Police Service of Scotland.

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 Police Service of Scotland has agreed to a consensual audit by the ICO of its processing of personal data.

1.4 A conference call was held on 18 August 2016 with representatives of Police Service of Scotland to identify and discuss the scope of the audit and to agree the schedule of interviews.

2. Scope of the audit

2.1 Following pre-audit discussions with Police Service of Scotland, it was agreed that the audit would focus on the following areas:

a. Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

3. Audit opinion

3.1 The purpose of the audit is to provide the Information Commissioner and Police Service of Scotland with an independent assurance of the extent to which Police Service of Scotland, 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	
Limited Assurance	There is a limited level of assurance that processes and procedures are in place and 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.

4. Summary of audit findings

4.1 Areas of good practice:

- All the Information Sharing Protocols (ISPs) reviewed during the audit set out the purpose for sharing personal data and the legal basis. The ISPs also capture how the personal data shared will be managed, especially the security requirements that must be in place.

- Police Service of Scotland (PSoS) has a security incident reporting process in place. This is supported by a standard Information Security Incident pro forma available to all staff on the intranet to report incidents, and a corporate log in place to record those incidents.

- The Performance Support and Delivery Unit within G Division has a comprehensive process in place for dealing with disclosure requests in relation to anti-social behaviour in terms of reviewing, recording and securely disclosing the relevant personal data.

4.2 Areas for improvement:

- There is an Information Management Checklist used by the Information Assurance Team to review new ISPs, but it is not part of a formal procedure and it not always used to review all new ISPs.

- Guidance is not in place to determine who is the appropriate authority within PSoS to sign off data sharing agreements.

- There are a number of legacy ISPs still in place which are yet to be reviewed to determine if they remain fit-for-purpose, or if they need to be updated.

- Logs are not always maintained in local business areas to record information requests received and subsequently the details of the disclosure made as a result of the request.

- Routine quality assurance checks are not undertaken on data inputted by operational staff into various PSoS systems.

- Assurance work is not undertaken by the Information Assurance Team regarding one-off disclosure activity within PSoS.

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 Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, Glasgow between 27 – 29 September 2016.

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 Sharing** – The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

Risk: The failure to design and operate appropriate data sharing controls is likely to contravene the principles of the Data Protection Act 1998, which may result in regulatory action, reputational damage to the organisation and damage or distress for those individuals who are the subject of the data.

Fair Processing Information

a1. Police Service of Scotland (PSoS) has an Information Charter in place that is publically available on the PSoS website.

a2. The charter provides details in broad terms of how PSoS will process personal data, how a data subject can access their personal data and the steps PSoS will take if it discloses personal data. It also provides advice on where an individual can get independent advice on data protection, and the relevant PSoS contact details.

a3. The Head of Information Management is responsible for ensuring the charter remains accurate, relevant and up-to-date in accordance with the Information Management Policy Framework. However, the practical arrangements of how this activity will be undertaken such as a review schedule, or the parties that should be involved in this review, are not documented.

Recommendation: The practical arrangements as to how the PSoS Information Charter will be managed to ensure it remains accurate, relevant and up-to-date should be documented.

Management Response: Accepted
Owner: Information Manager (Disclosure)
Implementation Date: 30/06/2017 and thereafter in accordance with review cycle established by the Information Manager (Disclosure)

a4. An example Information Sharing Protocol (ISP) was provided between PSoS and NHS Boards in Scotland for the purposes of the provision of healthcare and forensic services for people in the care of the police. The ISP included the following in regards to fair processing information:

- Definition of consent;
- Obtaining consent;
- Refused and withdrawn consent;
- Sharing information without consent;
- How to provide fair processing information to service users.

a5. In cases where an individual in police custody requires medical attention, it was reported that individuals are informed that their personal information will be shared with a health professional at the point of referral.

a6. In circumstances where the health professional requires access to the individual's health record, it was reported that consent is obtained. However, this consent is not recorded.

Recommendation: Where consent is obtained by Police Officers for health professionals to gain access to the individual's medical record, ensure a record of the consent is kept.

Management Response: Reject. Paragraph **a6** is unclear about which records are being accessed – NHS medical records, or police custody care and welfare questions/responses. An officer cannot obtain consent on behalf of NHS staff; and the responses to the vulnerability assessment are not medical questions/records.

The healthcare information provided by a custody is recorded in the vulnerability assessment section of the relevant prisoner processing system. This is free text and is passed verbally to the Health Care Professional (HCP) in accordance with existing ISP/SOP protocols. The information is recorded on the prisoner's custody record but the fact that it has been shared with NHS is not, unless it forms part of a custodial care plan, where a specific response to a vulnerability question provides a medically relevant response that requires medical intervention.

This area of information sharing is covered by verbal disclosures being in line with SOPs, as indicated at **a51**.

The incoming National Custody System presents an opportunity to establish additional functionality to record the transaction, if required. The national ISP which supports the Healthcare & Forensic Medical Service has been approved and signed off by Police Scotland ISP leads.

The HCP obtains consent at the beginning of any subsequent healthcare assessment and records the response(s) in the NHS IT system (ADASTRA). Police staff are not, and should not be, involved in this process.

a7. Whilst the majority of information shared by PSoS is under an enactment or covered by a relevant exemption, there are circumstances in which individual consent is relied upon to share personal information with partners in the information sharing agreement (ISA). However, not all ISAs include information regarding the requirement for parties to provide fair processing information to individuals and obtain consent where necessary.

Recommendations: a) Where appropriate, ensure ISAs include the requirement to provide fair processing and obtain consent.

Management Response: Accepted. The SOP, Template & Guidance for IM staff will be updated accordingly.
Owner: Head of Information Management
Implementation Date: 30/06/2017

b) Fair processing information provided and consent obtained should be recorded for audit and monitoring purposes.

Management Response: Accepted. The method of recording will be defined in ISAs where appropriate for SPOCs to implement and supervise.
Owner: SPOCs for each ISA
Implementation Date: 30/06/2017

<u>Information Sharing Agreements and Logs</u>

a8. PSoS has an Information Sharing standard operating procedure (SOP) which requires an ISA to be put in place when systematically sharing personal data with third parties. The SOP provides guidance on who is responsible for an ISA and the information that must be included when drafting an ISA. The SOP was due for a review in 2014.

Recommendation: As previously recommended in Audit 1, ensure the Information Sharing SOP is reviewed and updated. All policies and SOPs should be reviewed on an annual basis.

Management Response: Partially accepted. In line with the PSoS response to the Audit 1 recommendation, the review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support. This will take into account the standard applied across Police Scotland, the balance of work between policy review and improvement activity, and the fact that a policy or SOP can be updated at any time in response to a change to the external environment.
Owner: Head of Information Management
Date for implementation: 30/06/2017

a9. There are high level contractual agreements in place with third parties who PSoS systematically share personal information with. The ISAs are referred to as ISPs. It was reported that PSoS has approximately 166 active ISPs in place.

a10. ISPs reviewed by auditors set out the purpose of the ISP, partners involved, the legislation which permits the sharing of personal information, information to be shared, the management of information, roles and responsibilities and the parties responsible for reviewing the ISP. Where appropriate, ISPs included additional information and guidance within the Appendices.

a11. Business areas within PSoS are responsible for drafting ISPs. This responsibility commonly sits with a member of the project or planning group.

a12. Whilst the Information Sharing SOP provides brief guidance to business areas about the headings that must be included in an ISP, there is no standardised ISP template. As a result, it was reported by business areas that newly drafted ISPs are based upon existing ISPs that have been created by the particular business area in the past for previous projects. This includes ISPs created by the legacy forces.

Recommendations: a) Create a standardised ISP template which clearly sets out the content that must be included in all ISPs. The template should be included in the Information Sharing SOP.

b) As part of the review on the Information Sharing SOP, include guidance regarding appropriate signatories.

Management Response: Accepted. A generic template will be created; headings are already contained in the Information Sharing Protocol SOP. Additional information on appropriate signatories will be included in the updated SOP, to further define the guidance in the ISP SOP.
Owner: Information Manager (Assurance)
Implementation Date: 30/06/2017

a13. Once an ISP has been drafted, the ISP must be sent to the Information Assurance Team (IAT). Information Assurance Officers (IAOs) are responsible for conducting a compliance check on the ISP before it is distributed to the parties.

a14. There are currently two IAOs responsible for reviewing ISPs once drafted. ISPs are reviewed to ensure the correct legal basis for sharing information has been identified and documented, the correct headings have been included and to ensure all parties are notified to the ICO. Whilst an IAO has developed an Information Management Checklist to ensure all key areas are checked whilst conducting a review, this is not used by all IAOs.

a15. Once the ISP has been reviewed, a copy of the ISP (which documents all amendments and comments made by IAOs) is retained; either within a folder or within a copy of the email sent with the response.

Recommendations: a) Create a formal procedure which documents the process to follow when reviewing ISPs. Supported guidance such as the Information Management Checklist should be included in the procedure to assist IAOs when conducting a review. Formalising the procedure would ensure ISP reviews are consistent across IAOs. The procedure would also act as a training tool for those IAOs waiting to be trained.

b) Ensure all reviewed ISPs and associated correspondence are maintained for audit and monitoring purposes.

Management Response: Accepted. IM will produce a standard process and guidance for staff for use by all IAOs and IM staff in relation to the creation, review and governance of ISPs.
Owner: Information Manager (Assurance)
Implementation Date: 30/06/2017

a16. It was reported by an IAO interviewed that once changes have been completed by the business area, a final compliance check of the final draft is carried out. Another IAO reported that all ISP reviews carried out were approved by the Information Assurance Manager (IAM) (this role is currently vacant) before being returned to the business area.

Recommendation: The requirement for an IAO to undertake a compliance check of the final draft of the ISP should be documented in the procedure recommended above. Ensure the approval process for ISPs reviews is reallocated to an appropriate member of the Information Management Team (IMT) whilst waiting for the replacement IAM.

Management Response: Accepted. Please refer to response to **a15**.

a17. The business area is responsible for ensuring the ISP is signed by all parties mentioned within the agreement. The partnership agreement guidance provides information about who has the authority to sign off agreements. For PSoS, Local ISPs must be signed off by a Chief Superintendent. National ISPs are signed off by an Assistant Chief Constable. For third parties, ISPs must be signed off by a Chief Executive or a Director.

Recommendation: see recommendation **a12**.

Management Response: **Accepted**. Please refer to response to **a12**.

a18. ISPs are held by the business area responsible for the particular ISP. A copy of the signed ISP is provided to IAT. The business area is responsible for reviewing the ISP. Review dates are documented in the ISP and are usually carried out by a Superintendent or Inspector. It was reported that there are some ISP reviews outstanding.

a19. A log of all ISPs currently in place is maintained by the IAT. The log details whether the ISP has been signed, business owner, subject, partners, title, signatories and date signed. The review dates for ISPs and outcomes are not recorded on the log. As a result there are ISPs recorded as active on the log, but which have come to an end following a review.

Recommendations: a) Ensure all ISPs are reviewed within the period specified within the ISP. All reviews carried out should be formally documented for audit and monitoring purposes.

b) Ensure review dates and outcomes are documented on the ISP register. The IAT should notify business areas when an ISP is due for a review and provide a timeframe in which the review should be completed and the outcome reported. This should be logged on the register and chased if no response is received.

Management Response: Accepted. The ISP register will be amended to include review dates as defined in each ISP and processes for prioritisation and allocation of IM staff resources, oversight/monitoring developed for IM.
Owner: Information Manager (Assurance)/SPOCs
Implementation Date: Register, SOPs and processes by 30/06/2017; reviews in progress by 31/12/2017

a20. The IAT also maintains a register which records details of legacy ISPs. It was reported by the IAO that both the current and legacy logs are not accessible to all IAOs.

a21. ISPs currently in place within the PSoS are recorded on the partnership agreement page on the staff intranet. It was reported that all legacy ISPs have been removed and added to the legacy register or updated and added to the current ISP register. However, during interviews, auditors observed that there are a number of legacy ISPs documented on the partnership agreement page. The IAO was unsure if they were active ISPs.

Recommendations: a) Ensure the ISP registers for both current and legacy ISPs are accessible to all relevant IAOs. This would allow all IAOs within the IAT to access the registers for information and update where necessary.

b) Review the partnership agreement webpage and identify all legacy ISPs. Review ISPs to determine if the ISP has been terminated or is active. If the ISP has been terminated, remove and add to the legacy register. If the ISP is active, review and update the ISP and record on the current ISP register.

Management Response: Accepted. A review and update of the Intranet Partnership Working area (content, function and process) will be undertaken. Working with Policy Support/ICT, will establish a single working area for all IAOs linked to but hidden from the published ISP register.
Owner: Information Manager (Assurance)
Implementation Date: 30/09/2017

a22. There are no audits carried out by the PSoS to ensure that third parties in receipt of PSoS personal information are adhering to the requirements set out within the ISP.

Recommendations: a) Review ISPs and include the right for PSoS to audit third parties receiving PSoS personal information. Conduct audits to ensure parties are adhering to the requirements set out in the ISP.

b) Audits carried out should be formally documented for monitoring purposes.

Management Response: Rejected. PSoS considers that partners are data controllers in their own right and therefore must manage their responsibilities in relation to the information and in adherence with the agreements in the ISP. In addition, it is considered impractical for partners to formally audit each other; each having no right of access to the other's business. However, PSoS considers that there is an opportunity for SPOCs to seek confirmation from partners that the requirements of an ISP are being adhered to and that the ISP review process that it has agreed to define gives a formal opportunity for partners to confirm their commitment to and adherence with the contents of an ISP.

Data Quality and Retention

a23. The majority of ISPs reviewed by auditors detail the type of information that is likely to be shared with third parties and the circumstances in which the personal data will be shared. Information likely to be shared consists of individual names, addresses, date of birth, criminal history and any additional details that may be relevant to the circumstances.

Recommendation: Ensure all ISPs include the type of personal information that is mostly likely to be shared as part of the agreement. ISPs should also include the specific circumstances in which the personal information will be shared.

Management Response: Accepted. This is included in some ISPs already. This requirement will be emphasised in SOP, template and guidance for IM staff.
Owner: Information Manager (Assurance)
Implementation Date: 30/06/2017

a24. It was reported by an IAO that they undertake checks to ensure that the personal information that has been identified as the type of information that will be shared under the ISP is proportionate. However, whilst the IAO interviewed confirmed carrying out proportionality checks to ensure data is minimised, this is not carried out across the IAT.

Recommendation: Personal information shared under the ISP should be minimised to an agreed data set. The requirement for IAO to carry out data minimisation checks should be included as part of the ISP review process and formally documented in the Information Management checklist. Please refer to recommendation **a14**.

Management Response: Accepted. Please refer to response to a14.

a25. There are a number of circumstances in which PSoS would systematically share information with third party organisations. Personal information may be released to NHS health professionals as a result of an individual in custody requiring medical attention, during a particular event i.e. Open Golf or T in the Park, or cases in which PSoS have carried out landlord registry checks for local councils. Police Intelligence is also released routinely to the Scottish Prison Service (SPS) when required.

a26. Individuals responsible for handling information disclosure requests are referred to as the Single Point of Contact or 'SPOC'. Contact details of the SPOC are detailed within the ISP to ensure all third parties are aware of who to contact.

a27. There are processes in place for dealing with the different types of request. However, these are not clearly documented in a procedure.

Recommendation: Each nominated SPOC should seek to follow best practice in creating a procedure which clearly details the processes to follow when handling an information request received under the ISP. This should also include the requirement to check the accuracy of information before released. Creating a procedure ensures requests are dealt with consistently.

Management Response: Partially Accepted. PSoS agrees that defined procedures should be in place to deal with requests in a consistent manner and will include this requirement in SOP and IM staff guidance and in guidance to SPOCs on a revised section of the Intranet. However it is impractical to check the accuracy of every piece of information prior to release. QA checks are carried out on systems where data is entered. Please refer to the management response to **a28**.
Owner: Information Manager (Assurance)
Implementation Date: 30/06/2017

a28. Personal information released as a result of an information request is retrieved from PSoS crime legacy systems, Criminal History System (CHS), Police National Computer (PNC) and the Scottish Intelligence Database (SID). The Information Resources team is responsible for inputting information onto crime legacy systems, CHS and PNC. It was reported that Information Resources carry out quality assurance checks to ensure data is inputted accurately; however, no evidence was provided to auditors to support this statement. Police Officers are responsible for inputting data into SID.

Recommendation: Ensure QA checks are carried out by operating centres to ensure information is entered into relevant systems correctly. Routine QA checks would ensure the accuracy of information held on PSoS systems.

Management Response: Partially Accept. Quality assurance of CHS, PNC, SID and other national applications are independently quality assured by the National Systems Support (NSS) department of Police Scotland. This department provides central oversight of data inputters and system users and undertake daily quality assurance activities in line with the organisation's data quality strategy, authored by NSS. All quality assurance activity is driven by an information risk register which is compiled and monitored for each system under the department's responsibility. Data quality checks are developed to mitigate organisational and system risk and prioritised by the level of risk.

The PSoS data governance and audit structures are under review to enhance the approach to governance and audit.

In response to the observation of SID data quality management; SID logs are entered by Police Officers, however this information is not available to the wider user community until it has been quality checked by a Local Intelligence Officer who will correct discrepancies and ensure the information provided in the log is appropriately linked to other entities on the database, as well as other policing systems. Thereafter NSS undertake additional checks across the database targeting specific areas of weakness or risk. As well as ensuring the data is corrected they will attempt to control future data inaccuracies as per the principles of quality assurance

It is also noted that The Crime registrar has responsibilities for quality relating to crime recording information and undertakes assurance activities and system audits.

In relation to data entry/recording of data, auditors viewed the processes in one area (IR) and took evidence in relation to its processes; a summary of quality assurance mechanisms in Edinburgh and Lothians and Scottish Borders divisions is provided to indicate levels of QA and audit activity in a different area, and thereafter the IR (West) improvement plan in relation to recommendation a28 is detailed.

Criminal Justice Operations - 24Hr Unit:
New-start staff have all their work quality checked until the mentor and supervisor sign them off as competent.

All bail orders are checked by supervisors/team leaders, especially extradition bails/ witness bails/IBU bails with manual updates/split condition bails.

All warrant cancellations are quality checked on PNC to verify the warrant(s) are removed. Spot checks of CHS are carried out on transaction histories, to ensure staff are using the correct transaction codes.

Reports are subject to a ZZP transaction which also acts as a quality check.

Locate/trace markers - we e-mail the submitting officer back with a copy of the PNC entry and use this as the quality check.

A paper trail is required for any update carried out on CHS/PNC - never on the strength of a phone call. Updates to CHS/PNC are quality checked either by the individual themselves or by a supervisor/team leader.

DAF prints show the updates that staff have carried out to PNC so that weed dates are amended.

Records Department:
Staff are responsible for their own quality checking of all updates on CHS/PNC. Team leaders carry out intermittent transaction history reports on CHS to ensure that this is being carried out. The frequency of these checks is determined by the workflow and capacity of the department.

A team leader carries out checks on all Recorded Police Warnings and Anti-Social Behaviour Fixed Penalty Notices carried out by staff to ensure they have been updated correctly and staff are notified of errors.

PNC Bureau:
Whenever we update PNC and CHS, we carry out a QC transaction to check the details. When processing a warrant, the offence details are recorded on the CHS system before processing the warrant onto UNIFI. When we cancel a warrant - we delete the marker from PNC and this is QC the following day. We then update UNIFI, again this is QC the following day when we run the daily cancellation list.

Vehicle markers are input by the ACR, we QC the information to ensure the details are correct. We also routinely check the vehicle information held is correct with a range of processes. Disqualified Drivers - we verify the disqualification details on both the court system and CHS and update PNC.

Orders and Interdicts - we use the PNC DAF's to ensure that the markers are scheduled to be removed on the correct date and then QC it is no longer live.

C3 IR
Staff members undergo a continuous development programme designed to address skill-gaps across the CHS discipline. Resource availability determines that the main focus of quality assurance is in developing competencies of inexperienced staff rather than performing specific routine checks on work processed by all staff, i.e. experienced or otherwise.

However, once initial training is delivered in CHS-related tasks, an operators' work is 100% quality checked until competency is proved. Quality checks will reduce to 50%

and subsequently to 10%, subject to accuracy being maintained, before sign off in the task is achieved.

The results of these checks are recorded daily within Quality Log task folders held on the shared drive, where a skills matrix is also maintained.

Plans are in place to incorporate routine sampling for all levels of staff, the results of which will be recorded via a dashboard system and fully evaluated to correspond with quarterly PDC staff meetings. Instigate by 2nd quarter of 2017.

In the meantime, in order to mitigate against further risks associated with limited QA resources, routine checks for all staff are being triggered when the system auto-generates daily audit reports (batch prints) to highlight recorded information which potentially may require further attention or investigation.
Owner: C3 IR
Implementation Date: 30/06/2017

a29. It was reported that information sharing requests are logged and recorded onto relevant systems. However, in the case where information is required to be disclosed to a health professional, it was unclear if a log of all the referrals submitted and details of the information shared is maintained.

Recommendation: Ensure all business areas responsible for handling specific types of information sharing requests maintain a log which details the type of request received, party submitting the request, reason for requiring the information to be shared and details of the information that has been released as a result of the request. The requirement to record the details of information sharing requests should be included in the formal procedure recommended at **a27**.

Management Response: Partially Accept. Legacy custody systems cannot run a report which details the healthcare referrals made - the new National Custody System (NCS) presents an opportunity to establish that functionality. The national ISP which supports the Healthcare & Forensic Medical Service has been approved by Police Scotland ISP leads and signed off nationally.

Subject to the response to recommendation **a6**, and the verbal disclosure proviso at **a51**, we are looking to establish the reporting functionality, hopefully in phase 2 of NCS, estimated for June 2017.
Owner: Criminal Justice Services Division
Implementation Date: 30/06/2017

a30. QA checks are not carried out on information disclosure requests handled by SPOCs in business areas.

Recommendation: Carry out regular QA checks on information sharing requests handled by SPOCs, to ensure that the data shared is relevant to the purposes it was requested for and proportionate. All QA checks carried out by business areas should be documented for audit and monitoring purposes.

Management Response: Accepted. IM will agree a schedule of compliance audits and an approach that focuses on the highest areas of information risk. This is dependent on resources being available in the highly challenging financial environment in which PSoS operates. Consequently, IM will also consider how QA can be integrated into procedures for information sharing with SPOCs at point of design and also during ISP reviews.
Owner: Head of Information Management

Implementation Date: 31/12/2017

a31. It was reported that the IAT began conducting an audit of divisions sharing information under anti-social behaviour legislation. The purpose of the audit was to ensure a similar procedure for disclosure was followed throughout divisions and the information shared was to a minimised standard. However, the audit was not completed.

Recommendation: Ensure the audit on information sharing under anti-social behaviour legislation is completed. Once completed, expand the approach and carry out information sharing audits in other substantial areas.

Management Response: Accepted. Please refer to response to **a30**.

a32. Whilst the majority of the ISPs reviewed by auditors set out the common rules to follow in relation to the retention of information shared, this is not included in all ISPs currently in place.

Recommendation: Make sure all ISPs include retention requirements to ensure personal information shared is not retained for any longer than is necessary. Creating a standardised ISP template would ensure all ISPs include all relevant requirements. Please refer to recommendation at **a12**.

Management Response: Accepted. Please refer to response to **a12**.

a33. ISPs state that information shared for the purposes set out in the agreement should not be kept for longer than is necessary. ISPs require third parties to retain information in accordance with their own retention schedule. However, no assurance is sought by PSoS to confirm the third party has a retention schedule in place and what the retention periods are.

Recommendation: Require third parties to provide PSoS with a copy of their retention schedule to ensure information is not kept any longer than necessary.

Management Response: Partially Accept. IM will ensure that the retention period for data shared with partners is known and included in ISPs. The requirement will be included in the updated SOP, template and guidance.
Owner: Information Manager (Assurance)/SPOCs
Implementation Date: 30/06/2017

a34. The majority of ISPs clearly set out disposal arrangements for information which is shared under the agreement. Manual data shared under the ISP should be cross shredded or destroyed as confidential waste. Media should be cut and destroyed and electronic data should be securely destroyed in line with the individual party’s destruction policy. However, similar to retention, not all ISPs clearly set out specific disposal arrangements.

a35. PSoS currently does not obtain assurance from partners that information shared is deleted or destroyed securely, once the purpose is no longer relevant.

Recommendation: a) Ensure specific disposal arrangements for both manual and electronic data shared is specified within all ISPs currently in place. Please refer to recommendation in **a14** and **a32** regarding the creation of a standardised ISP template.

b) Guarantees and assurances should be sought to confirm that partners in recipient of PSoS information have securely deleted/destroyed information shared.

Management Response: Partially Accept. Disposal arrangements are generally included in new ISPs. This will be a mandatory requirement and will be included in a standardised ISP template. Confirmation of secure destruction will be built into ISP review processes and IA audit schedule.
Owner: Information Manager (Assurance)/SPOCs
Implementation Date: 31/12/2017

Security

a36. PSoS has an Information Sharing SOP in place that includes examples of standard management clauses in relation to security. This was last reviewed in October 2013.

Recommendation: see recommendation **a8**.

Management Response: Partially Accepted. Please refer to response to **a8**.

a37. All of the example ISPs that were provided included the required information security clauses and had added further detail where necessary, such as when a Code of Connection for access to PSoS electronic systems was required.

a38. There is also a Requests for Personal Information from External Bodies SOP in place which was last reviewed in July 2013. This details the means by which requests can be received securely and how subsequent police data should remain secure during transmission.

Recommendation: see recommendation **a8**.
Management Response: Partially Accepted. Please refer to response to **a8**.

a39. A Security Incident Reporting and Management SOP, published in November 2013, provides the framework for the management of information security incidents. It outlines the responsibilities of both operational staff and the Information Management Team (IMT) in handling an incident. It sets out a requirement to log incidents, and ultimately report outcomes and mitigations to the SIRO.

Recommendation: see recommendation **a8**.
Management Response: Partially Accepted. Please refer to response to a8.

a40. There is a standard Information Security Incident reporting pro forma available on the PSoS intranet. Staff have to provide details of the incident and any mitigation measures already taken.

a41. A Corporate Log is maintained by IAT of all reported information security incidents.

a42. There is an Information Security Manager in place within the IMT. Part of their responsibilities includes commissioning an annual programme of information security and assurances audits.

a43. The audit programme for 2015-16 included a number of audits in relation to data sharing. Audits have been undertaken on the use by staff of social networking sites for business purposes and the access partners are given to police systems.

a44. Reports are normally delivered back to the business area IAO to agree and implement recommendations; if a report is of sufficient seriousness it will go to the relevant Head of Division, and ultimately the Force Governance Board if major risk is identified.

a45. It was also reported that members of the IMT hold a weekly meeting with a standard agenda that includes discussions around data sharing and security.

Recommendation: The Information Management team weekly meeting should have a specific agenda point covering data sharing, focusing on any information security risks arising from current activity.

Management Response: Accepted. Please note that IM holds weekly meetings for its Disclosure and Assurance Teams. This suggestion is accepted for the Information Assurance team which is part of the wider Information Management department.
Owner: Head of Information Management
Implementation Date: Implemented

a46. In terms of systematic data sharing IAOs will review draft ISPs, specifically to evaluate the security controls in place. Advice and guidance will be provided to the owner of the ISP where necessary.

Recommendation: see recommendation **a15**.

Management Response: Accepted. Please refer to response to **a15**.

a47. It was reported that when outside agencies (such as local authorities) are granted access to police systems, IAOs will review their IT security controls during the set-up of the system. They will also review proposed access rights of users at the partner agency to ensure they are proportionate and necessary.

a48. IAT does not undertake any compliance work around the security controls in place for one-off disclosures of police data to third parties.

Recommendation: Ensure the Information Assurance Team undertake some assurance work to review the security procedures in place for one-off disclosure activity.

Management Response: Accepted. IM will agree a schedule of compliance audits and an approach that focuses on the highest areas of risk.
Owner: Head of Information Management
Implementation Date: 31/12/2017

a49. Through observation of both systematic and one-off data sharing activity PSoS demonstrated awareness of the need to verify a request as legitimate before they commenced processing it. Requests normally had to be receiving in writing, and in some cases had to be received from a specific nominated individual at a partner organisation.

Recommendation: As we only observed activity in a limited number of areas, PSoS should ensure all operational teams have assessed their own processes in managing requests and this is appropriate to the risk level of preventing an inappropriate disclosure. Please refer to recommendation **a27** for additional detail.

Management Response: Accepted. In addition to the response to **a27** and **a15**, PSoS will seek to develop and relaunch the 'principles' of information sharing on the Intranet, providing guidance on good practice, FAQs, etc. to accompany revised SOPs and templates as well as good practice for one-off disclosures.

Thereafter, targeted communication and tasking (where appropriate) using established structures, e.g. Criminal Justice Services Division Continuous Improvement Board.
Owner: Information Manager (Assurance)

Implementation Date: 30/09/2017

a50. One example was identified when a partner organisation had previously been required to complete a specific pro forma to request information, but now just sent an email request to the responsible PSoS team.

Recommendation: Operational teams should be using standard pro-formas where possible to ensure consistency in initial logging and review of requests for PSoS data.

Management Response: Partially Accepted. PSoS accepts that consistency in accepting, recording and sharing/refusing information requests is essential, however each ISP/disclosure process may require a different solution (for example a form or a standard e-mail template or a data sharing portal) and therefore each ISP and/or procedure should specify the appropriate format that SPOCs should thereafter adhere to.
Owner: Information Manager (Assurance)/SPOCs
Implementation Date: 30/06/2017

a51. Our observations also demonstrated PSoS were conscious of security requirements during transmission of data. The vast majority of disclosures were only made in writing, either through secure email, post or physical collection. In most cases where verbal disclosures were made this was in line with the SOP that governed the process.

Recommendation: see recommendation **a49**.

Management Response: Accepted. Please refer to response to **a49**.

a52. As a result of the Risk & Concern Project, PSoS have taken the decision to improve the security around transmission of data from Concern Hubs to partner organisations by implementing Egress Switch functionality. Egress Switch requires both sender and recipient to enter unique log-in details, and encrypts data in transit.

Disclosures

a53. There is a Requests for Personal Information from External Bodies SOP in place which was last reviewed in July 2013. It outlines what the process police officers and staff should adopt when requesting personal data from non-police bodies where there is not an ISP in place.

Recommendation: see recommendation **a8**.

Management Response: Partially Accepted. Please refer to response to **a8**.

a54. The SOP outlines potential legal gateways (largely Section 29(3) of the DPA for the Police) and it details some of the operational requirements around requesting information under Section 29(3).

a55. There is also a Public Interest Disclosure SOP in place. It is not clear who owns this SOP or when it was last reviewed but it sets out the process for disclosing sensitive personal information when disclosure is necessary in the public interest, and when there are no specific statutory powers or relevant PSoS procedures.

Recommendation: see recommendation **a8**.

Management Response: Partially Accepted. Please refer to response to **a8**.

a56. The SOP guides officers and staff as to how they can reach a decision regarding a public interest disclosure and how practically they should make the disclosure. The ultimate decision to disclose in the public interest must still be made by an officer of the rank of Superintendent or above. There is also the requirement that the individual concerned should also be informed in writing that sensitive personal information about them will be, or has been disclosed by PSoS.

a57. Observation of one-off disclosure activity was mainly focused on the disclosure of information relating to crime/road traffic accident reports and confirmation of warrants in place to solicitors and insurance companies.

a58. Both of the above activities have written processes in place, although the confirmation of a warrants process has not been reviewed since 2008.

Recommendation: see recommendation **a8**.

Management Response: Accept. A full end to end review of the existing guidance on the handling of "solicitor's letters" will be undertaken - from the receipt and processing of the initial enquiry, to the release of information and supportive quality controls. C3 IR will work with Information Management to ensure a corporate approach with other force areas and that all aspects of this process are fully compliant with legislative guidance and SOP pertaining to Information Sharing. Following the review - process guidance will be circulated to IR operators and formal copy retained within the Departmental shared drive for reference. In order to ensure that the process remains in line with the Guidance, we will set up a review schedule for the process, to match the review timelines of the SOPs.
Owner: C3
Implementation Date: 14/02/2017

a59. Staff within the Information Resources (IR) Team are part of the national Contact, Command and Control Division (known as C3). The team (based in Glasgow) covers activity in the West Command area. It was reported to auditors' onsite that the team follows its own processes for dealing with requests from third parties / disclosures, and there is no joint approach or mechanism to coordinate activity with other Command areas.

Recommendation: PSoS should seek to review best practice across the Command areas and implement a standard operational process for dealing with request from third parties / disclosure requests.

Management Response: Accept. Existing legacy force processes were set up in line with the legacy demand requirements and RTC data is received via Force Form 442 - which is an 8 page document. Guidance on what data can be released is based on the information contained within the form relating to non-injury and injury incidents. Note: if the enquiry is from a member of the public then personal info is redacted so that only name, insurance details and the info relating to date/time locus of accident is shared.
We acknowledge a variance across the legacy areas in how abstracts are processed across Scotland - these different processes have evolved according to the local data systems used and there are also variances in demand, staffing and historic local agreements. However despite these differences and the absence of a single national structure for this work - the data released still complies with relevant SOPS and legislative guidance. Also, we do consult with "regional" Information Management disclosure SPOCS if we receive any ad hoc enquires unrelated to the abstract process, in order to ensure that we remain compliant.
The Abstract SOP is due for renewal and C3 will assist Information Management with that review when called upon to contribute. Whilst C3 can contribute to a national review

of the RTC Abstract process to identify best practice and establish a single corporate approach, it should be understood that IR has no authority or remit to impose change on a national basis. However, C3 will coordinate the formation of a short-life WG, made up of C3/IM/CJ/IR to move towards discharge or partial discharge pending future organisational change.
Owner: C3
Implementation Date: 28/02/2017

a60. Abstracts of Crime/Road Traffic Accidents are released to insurance companies or solicitors with the minimal personal data required to pursue an insurance claim or legal proceedings.

a61. The C3 West Command IR keep a log of requests in terms of recording if they have received a fee to process to request, but do not keep an actual log of the disclosures made and the rationale behind them. It was also not clear if any quality assurance is undertaken on the disclosures made.

Recommendation: A log designed to specifically record all the requests received should be created which captures the detail as to what personal data has been disclosed and the rationale as to why. Sample checking of disclosures should also be undertaken to ensure quality and consistency in disclosures being made.

Management Response: Accept. Specifically relating to the existing 442 RTC database - it is a local in-house system. There are limitations in the design of the database as it was not set up to manage the end-to-end abstract process and to record quality checking activity.

When the mail arrives, all abstract and precognition requests are reviewed and the operator will perform checks to ensure:

- the legitimacy of the request
- that payment is correct
- the incident relates to our regional area
- the query is sufficiently detailed to carry out a search

Details released will pertain to whether the enquiry is from an insurance company/solicitor or from a member of the public. Guidance of what info is released is strictly applied.

In addition, 100% Quality checking is undertaken on staff learning the process - and they are deemed to competent when the 95% quality mark has been consistently attained. Checking is undertaken by the team leader and quality sheets produced for operator feedback.

C3 IR is currently in talks with ICT to review our processes with a view to develop a new electronic procedure to manage RTC business and to enhance governance.
Owner: C3
Implementation Date: ICT dependent

a62. A log is kept of all requests to confirm the existence of a warrant, to provide justification if evidence is requested as to why a search was completed on an individual on the Police National Database.

a63. Another area where PSoS process a large volume of disclosures is sharing information about anti-social behaviour with local authorities, housing associations and registered social landlords, under the provision of the Antisocial Behaviour etc. (Scotland) Act 2004.

a64. Requests for personal data in relation to anti-social behaviour in the Greater Glasgow area are managed by the Performance Support and Delivery Unit within G Division.

a65. This Unit keeps a clear log of all requests received, who dealt with the request, what personal data was released and the rationale as to why. The process is governed by specific pro forma, requiring the requestor to set out what personal data they want, the justification and the time period the request covers. The ultimate decision to disclose is made by the Area Commander in the local area that receives and actually discloses the data.

a66. The Unit staff are trained to undertake data quality assessments on the information shared with Local Area Commanders. It was unclear from the site visit if any independent reviews are undertaken on the decision these staff make around disclosure.

Recommendation: Sample checking of disclosures should also be undertaken to ensure quality and consistency in information being shared with the Local Area Commander for disclosure.

Management Response: Partially Accept. Please refer to the response to **a30**.

As an organisation, work is ongoing to bring in quality assurance checks for divisions to assure quality at a local level and consistency at a national level. In addition, Local Policing will seek to work with divisions in terms of process and quality of product in anticipation of this being implemented.
Owner: Chief Inspector Local Policing
Implementation Date: 30/06/2017

a67. We also observed sharing of data in another Division in relation to anti-social behaviour. It was reported the team in this Division were not adhering to a specific national SOP or process. This team also only kept a very basic log of requests, which did not provide any rationale for why certain personal data was disclosed.

Recommendation: see recommendation **a59.**

Management Response: Partially Accepted. The revised Information Sharing SOP, guidance and Intranet information will support the development and use of standardised working practices where appropriate.

Please also refer to the response to **a30**.
Owner: Head of Information Management
Implementation Date: 31/12/2017

a68. PSoS have in place a number of Concern Hubs to manage the flow of information recorded on the Vulnerable Persons Database, and determine how it should be disclosed to relevant partners.

a69. A major project has been undertaken during the first half of 2016 to standardise the operational model and process across the Concern Hubs in the 13 Divisions of PSoS. The Project worked with four Divisional Concern Hubs to achieve best practice, which includes formalised national guidance on research and disclosures.

a70. An evaluation report will be presented to the PSoS Senior Management Team before the end of 2016 for review and to seek the resource to support the implementation of the enhanced operational model and process across the remaining nine Divisional Concern Hubs.

Recommendation: The best practice operational model for the Concern Hubs should be implemented across all Divisions as soon as practicable.

PSoS should also consider if any lessons learned or elements of the best practice model developed can be introduced into other data sharing activity.

Management Response: Accepted. The training schedule has been developed and will roll out during 2017.
Owner: SCD
Implementation Date: Starting December 2016

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

7.3 Any queries regarding this report should be directed to [redacted] Engagement Lead Auditor, ICO Good Practice.

7.4 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. [redacted] Records Manager was particularly helpful in organising the audit.

Appendix A

Detailed findings and action plan

Action plan and progress

Recommendation	**Agreed action, date and owner**	**Progress at 3 months** Describe the status and action taken.	**Progress at 6 months** Describe the status and action taken.
a3. The practical arrangements as to how the PSoS Information Charter will be managed to ensure it remains accurate, relevant and up-to-date should be documented.	**Management Response: Accepted** **Owner:** Information Manager (Disclosure) **Implementation Date:** 30/06/2017 and thereafter in accordance with review cycle established by the Information Manager (Disclosure).		
a6. Where consent is obtained by Police Officers for health professionals to gain access to the individual's medical record, ensure a record of the consent is kept.	**Management Response: Reject.** Paragraph **a6** is unclear about which records are being accessed – NHS medical records, or police custody care and welfare questions/responses. An officer cannot obtain consent on behalf of NHS staff; and the responses to the vulnerability assessment are not medical		

	questions/records. The healthcare information provided by a custody is recorded in the vulnerability assessment section of the relevant prisoner processing system. This is free text and is passed verbally to the Health Care Professional (HCP) in accordance with existing ISP/SOP protocols. The information is recorded on the prisoner's custody record but the fact that it has been shared with NHS is not, unless it forms part of a custodial care plan, where a specific response to a vulnerability question provides a medically relevant response that requires medical intervention. This area of information sharing is covered by verbal disclosures being in line with SOPs, as indicated at **a51**. The incoming National Custody System presents an opportunity to establish additional functionality to		

	record the transaction, if required. The national ISP which supports the Healthcare & Forensic Medical Service has been approved and signed off by Police Scotland ISP leads. The HCP obtains consent at the beginning of any subsequent healthcare assessment and records the response(s) in the NHS IT system (ADASTRA). Police staff are not, and should not be, involved in this process.		
a7. a) Where appropriate, ensure ISAs include the requirement to provide fair processing and obtain consent. b) Fair processing information provided and consent obtained should be recorded for audit and monitoring purposes.	**Management Response: Accepted.** The SOP, Template & Guidance for IM staff will be updated accordingly. **Owner:** Head of Information Management **Implementation Date:** 30/06/2017 **Management Response: Accepted**. The method of recording will be defined in ISAs where appropriate for SPOCs to implement and supervise. **Owner:** SPOCs for each ISA		

	Implementation Date: 30/06/2017		
a8. As previously recommended in Audit 1, ensure the Information Sharing SOP is reviewed and updated. All policies and SOPs should be reviewed on an annual basis.	**Management Response:** **Partially accepted**. In line with the PSoS response to the Audit 1 recommendation, the review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support. This will take into account the standard applied across Police Scotland, the balance of work between policy review and improvement activity, and the fact that a policy or SOP can be updated at any time in response to a change to the external environment. **Owner:** Head of Information Management **Date for implementation:** 30/06/2017		
a12. a) Create a standardised ISP template which clearly sets out the content that must be included in all ISPs. The template should be included in the	**Management Response:** **Accepted.** A generic template will be created; headings are already contained in the Information Sharing Protocol SOP. Additional information on appropriate signatories will		

Information Sharing SOP. b) As part of the review on the Information Sharing SOP, include guidance regarding appropriate signatories.	be included in the updated SOP, to further define the guidance in the ISP SOP. **Owner:** Information Manager (Assurance) **Implementation Date:** 30/06/2017		
a14/15. a) Create a formal procedure which documents the process to follow when reviewing ISPs. Supported guidance such as the Information Management Checklist should be included in the procedure to assist IAOs when conducting a review. Formalising the procedure would ensure ISP reviews are consistent across IAOs. The procedure would also act as a training tool for those IAOs waiting to be trained. b) Ensure all reviewed ISPs and associated	**Management Response: Accepted.** IM will produce a standard process and guidance for staff for use by all IAOs and IM staff in relation to the creation, review and governance of ISPs. **Owner:** Information Manager (Assurance) **Implementation Date:** 30/06/2017		

correspondence are maintained for audit and monitoring purposes.			
a16. The requirement for an IAO to undertake a compliance check of the final draft of the ISP should be documented in the procedure recommended above. Ensure the approval process for ISPs reviews is reallocated to an appropriate member of the Information Management Team (IMT) whilst waiting for the replacement IAM.	**Management Response: Accepted.** Please refer to response to **a15**.		
a17. See recommendation **a12**.	**Management Response**: **Accepted**. Please refer to response to **a12**.		
a18/19. a) Ensure all ISPs are reviewed within the period specified within the ISP. All reviews carried out should be formally	**Management Response: Accepted.** The ISP register will be amended to include review dates as defined in each ISP and processes for prioritisation and allocation		

documented for audit and monitoring purposes. b) Ensure review dates and outcomes are documented on the ISP register. The IAT should notify business areas when an ISP is due for a review and provide a timeframe in which the review should be completed and the outcome reported. This should be logged on the register and chased if no response is received.	of IM staff resources, oversight/monitoring developed for IM. **Owner:** Information Manager (Assurance)/SPOCs **Implementation Date:** Register, SOPs and processes by 30/06/2017; reviews in progress by 31/12/2017		
a20/21. a) Ensure the ISP registers for both current and legacy ISPs are accessible to all relevant IAOs. This would allow all IAOs within the IAT to access the registers for information and update where necessary. b) Review the	**Management Response:** **Accepted**. A review and update of the Intranet Partnership Working area (content, function and process) will be undertaken. Working with Policy Support/ICT, will establish a single working area for all IAOs linked to but hidden from the published ISP register. **Owner:** Information		

partnership agreement webpage and identify all legacy ISPs. Review ISPs to determine if the ISP has been terminated or is active. If the ISP has been terminated, remove and add to the legacy register. If the ISP is active, review and update the ISP and record on the current ISP register.	Manager (Assurance) **Implementation Date:** 30/09/2017		
a22. a) Review ISPs and include the right for PSoS to audit third parties receiving PSoS personal information. Conduct audits to ensure parties are adhering to the requirements set out in the ISP. b) Audits carried out should be formally documented for monitoring purposes.	**Management Response: Rejected.** PSoS considers that partners are data controllers in their own right and therefore must manage their responsibilities in relation to the information and in adherence with the agreements in the ISP. In addition, it is considered impractical for partners to formally audit each other; each having no right of access to the other's business. However, PSoS considers that there is an opportunity for SPOCs to seek confirmation from partners that the		

	requirements of an ISP are being adhered to and that the ISP review process that it has agreed to define gives a formal opportunity for partners to confirm their commitment to and adherence with the contents of an ISP.		
a23. Ensure all ISPs include the type of personal information that is mostly likely to be shared as part of the agreement. ISPs should also include the specific circumstances in which the personal information will be shared.	**Management Response: Accepted**. This is included in some ISPs already. This requirement will be emphasised in SOP, template and guidance for IM staff. **Owner:** Information Manager (Assurance) **Implementation Date:** 30/06/2017		
a24. Personal information shared under the ISP should be minimised to an agreed data set. The requirement for IAO to carry out data minimisation checks should be included as part of the ISP review process and formally documented in the Information	**Management Response: Accepted.** Please refer to response to **a14.**		

Management checklist. Please refer to recommendation **a14**.			
a27. Each nominated SPOC should seek to follow best practice in creating a procedure which clearly details the processes to follow when handling an information request received under the ISP. This should also include the requirement to check the accuracy of information before released. Creating a procedure ensures requests are dealt with consistently.	**Management Response: Partially Accepted.** PSoS agrees that defined procedures should be in place to deal with requests in a consistent manner and will include this requirement in SOP and IM staff guidance and in guidance to SPOCs on a revised section of the Intranet. However it is impractical to check the accuracy of every piece of information prior to release. QA checks are carried out on systems where data is entered. Please refer to the management response to **a28.** **Owner:** Information Manager (Assurance) **Implementation Date:** 30/06/2017		
a28. Ensure QA checks are carried out by operating centres to ensure information is entered into relevant systems correctly. Routine QA checks	**Management Response: Partially Accept.** Quality assurance of CHS, PNC, SID and other national applications are independently quality assured by the National		

would ensure the accuracy of information held on PSoS systems.	Systems Support (NSS) department of Police Scotland. This department provides central oversight of data inputters and system users and undertake daily quality assurance activities in line with the organisation's data quality strategy, authored by NSS. All quality assurance activity is driven by an information risk register which is compiled and monitored for each system under the department's responsibility. Data quality checks are developed to mitigate organisational and system risk and prioritised by the level of risk. The PSoS data governance and audit structures are under review to enhance the approach to governance and audit. In response to the observation of SID data quality management; SID logs are entered by Police Officers, however this		

	information is not available to the wider user community until it has been quality checked by a Local Intelligence Officer who will correct discrepancies and ensure the information provided in the log is appropriately linked to other entities on the database, as well as other policing systems. Thereafter NSS undertake additional checks across the database targeting specific areas of weakness or risk. As well as ensuring the data is corrected they will attempt to control future data inaccuracies as per the principles of quality assurance It is also noted that The Crime registrar has responsibilities for quality relating to crime recording information and undertakes assurance activities and system audits. In relation to data entry/recording of data,		

	auditors viewed the processes in one area (IR) and took evidence in relation to its processes; a summary of quality assurance mechanisms in Edinburgh and Lothians and Scottish Borders divisions is provided to indicate levels of QA and audit activity in a different area, and thereafter the IR (West) improvement plan in relation to recommendation **a28** is detailed. Criminal Justice Operations - 24Hr Unit: New-start staff have all their work quality checked until the mentor and supervisor sign them off as competent. All bail orders are checked by supervisors/team leaders, especially extradition bails/ witness bails/IBU bails with manual updates/split condition bails. All warrant cancellations are quality checked on PNC to verify the warrant(s) are removed. Spot checks of		

	CHS are carried out on transaction histories, to ensure staff are using the correct transaction codes. Reports are subject to a ZZP transaction which also acts as a quality check. Locate/trace markers - we e-mail the submitting officer back with a copy of the PNC entry and use this as the quality check. A paper trail is required for any update carried out on CHS/PNC - never on the strength of a phone call. Updates to CHS/PNC are quality checked either by the individual themselves or by a supervisor/team leader. DAF prints show the updates that staff have carried out to PNC so that weed dates are amended. Records Department: Staff are responsible for their own quality checking of all updates on CHS/PNC. Team		

	leaders carry out intermittent transaction history reports on CHS to ensure that this is being carried out. The frequency of these checks is determined by the workflow and capacity of the department. A team leader carries out checks on all Recorded Police Warnings and Anti-Social Behaviour Fixed Penalty Notices carried out by staff to ensure they have been updated correctly and staff are notified of errors. PNC Bureau: Whenever we update PNC and CHS, we carry out a QC transaction to check the details. When processing a warrant, the offence details are recorded on the CHS system before processing the warrant onto UNIFI. When we cancel a warrant - we delete the marker from PNC and this is QC the following day. We then update UNIFI, again this is QC the following day when we run the daily cancellation list.		

	Vehicle markers are input by the ACR, we QC the information to ensure the details are correct. We also routinely check the vehicle information held is correct with a range of processes. Disqualified Drivers - we verify the disqualification details on both the court system and CHS and update PNC. Orders and Interdicts - we use the PNC DAF's to ensure that the markers are scheduled to be removed on the correct date and then QC it is no longer live. C3 IR Staff members undergo a continuous development programme designed to address skill-gaps across the CHS discipline. Resource availability determines that the main focus of quality assurance is in developing competencies of inexperienced staff rather than performing specific		

	routine checks on work processed by all staff, i.e. experienced or otherwise. However, once initial training is delivered in CHS-related tasks, an operators' work is 100% quality checked until competency is proved. Quality checks will reduce to 50% and subsequently to 10%, subject to accuracy being maintained, before sign off in the task is achieved. The results of these checks are recorded daily within Quality Log task folders held on the shared drive, where a skills matrix is also maintained. Plans are in place to incorporate routine sampling for all levels of staff, the results of which will be recorded via a dashboard system and fully evaluated to correspond with quarterly PDC staff meetings. Instigate by 2nd quarter of 2017.		

	In the meantime, in order to mitigate against further risks associated with limited QA resources, routine checks for all staff are being triggered when the system auto-generates daily audit reports (batch prints) to highlight recorded information which potentially may require further attention or investigation. **Owner:** C3 IR **Implementation Date:** 30/06/2017		
a29. Ensure all business areas responsible for handling specific types of information sharing requests maintain a log which details the type of request received, party submitting the request, reason for requiring the information to be shared and details of the information that has been released as a result of the request. The requirement to	**Management Response: Partially Accept.** Legacy custody systems cannot run a report which details the healthcare referrals made - the new National Custody System (NCS) presents an opportunity to establish that functionality. The national ISP which supports the Healthcare & Forensic Medical Service has been approved by Police Scotland ISP leads and signed off nationally. Subject to the response to recommendation **a6**, and the		

record the details of information sharing requests should be included in the formal procedure recommended at **a27.**	verbal disclosure proviso at **a51**, we are looking to establish the reporting functionality, hopefully in phase 2 of NCS, estimated for June 2017. **Owner:** Criminal Justice Services Division **Implementation Date:** 30/06/2017		
a30. Carry out regular QA checks on information sharing requests handled by SPOCs, to ensure that the data shared is relevant to the purposes it was requested for and proportionate. All QA checks carried out by business areas should be documented for audit and monitoring purposes.	**Management Response:** **Accepted.** IM will agree a schedule of compliance audits and an approach that focuses on the highest areas of information risk. This is dependent on resources being available in the highly challenging financial environment in which PSoS operates. Consequently, IM will also consider how QA can be integrated into procedures for information sharing with SPOCs at point of design and also during ISP reviews. **Owner:** Head of Information Management **Implementation Date:** 31/12/2017		
a31. Ensure the audit on information sharing	**Management Response:** **Accepted.** Please refer to		

under anti-social behaviour legislation is completed. Once completed, expand the approach and carry out information sharing audits in other substantial areas.	response to **a30.**		
a32. Make sure all ISPs include retention requirements to ensure personal information shared is not retained for any longer than is necessary. Creating a standardised ISP template would ensure all ISPs include all relevant requirements. Please refer to recommendation at **a12.**	**Management Response: Accepted.** Please refer to response to **a12.**		
a33. Require third parties to provide PSoS with a copy of their retention schedule to ensure information is not kept any longer than necessary.	**Management Response: Partially Accept.** IM will ensure that the retention period for data shared with partners is known and included in ISPs. The requirement will be included in the updated SOP, template and guidance. **Owner:** Information		

	Manager (Assurance)/SPOCs **Implementation Date:** 30/06/2017		
a34/35. a) Ensure specific disposal arrangements for both manual and electronic data shared is specified within all ISPs currently in place. Please refer to recommendation in **a14** and **a32** regarding the creation of a standardised ISP template. b) Guarantees and assurances should be sought to confirm that partners in recipient of PSoS information have securely deleted/destroyed information shared.	**Management Response: Partially Accept.** Disposal arrangements are generally included in new ISPs. This will be a mandatory requirement and will be included in a standardised ISP template. Confirmation of secure destruction will be built into ISP review processes and IA audit schedule. **Owner:** Information Manager **(Assurance)/SPOCs** **Implementation Date:** 31/12/2017		
a36. See recommendation **a8.**	**Management Response: Partially Accepted.** Please refer to response to **a8.**		
a38. See recommendation **a8.**	**Management Response: Partially Accepted.** Please refer to response to **a8.**		
a39. See recommendation **a8.**	**Management Response: Partially Accepted.** Please		

	refer to response to **a8.**		
a45. The Information Management team weekly meeting should have a specific agenda point covering data sharing, focusing on any information security risks arising from current activity.	**Management Response: Accepted.** Please note that IM holds weekly meetings for its Disclosure and Assurance Teams. This suggestion is accepted for the Information Assurance team which is part of the wider Information Management department. **Owner:** Head of Information Management **Implementation Date:** Implemented		
a46. See recommendation **a15.**	**Management Response: Accepted.** Please refer to response to **a15.**		
a48. Ensure the Information Assurance Team undertake some assurance work to review the security procedures in place for one-off disclosure activity.	**Management Response: Accepted.** IM will agree a schedule of compliance audits and an approach that focuses on the highest areas of risk. **Owner:** Head of Information Management **Implementation Date:** 31/12/2017		
a49. As we only observed activity in a limited number of areas, PSoS should ensure all operational teams have assessed	**Management Response: Accepted.** In addition to the response to **a27** and **a15,** PSoS will seek to develop and relaunch the 'principles' of information sharing on the		

their own processes in managing requests and this is appropriate to the risk level of preventing an inappropriate disclosure. Please refer to recommendation **a27** for additional detail.	Intranet, providing guidance on good practice, FAQs, etc. to accompany revised SOPs and templates as well as good practice for one-off disclosures. Thereafter, targeted communication and tasking (where appropriate) using established structures, e.g. Criminal Justice Services Division Continuous Improvement Board. **Owner:** Information Manager (Assurance) **Implementation Date:** 30/09/2017		
a50. Operational teams should be using standard pro-formas where possible to ensure consistency in initial logging and review of requests for PSoS data.	**Management Response: Partially Accepted.** PSoS accepts that consistency in accepting, recording and sharing/refusing information requests is essential, however each ISP/disclosure process may require a different solution (for example a form or a standard e-mail template or a data sharing portal) and therefore each ISP and/or procedure should specify the appropriate format that		

	SPOCs should thereafter adhere too. **Owner:** Information Manager (Assurance)/SPOCs **Implementation Date:** 30/06/2017		
a51. See recommendation **a49.**	**Management Response: Accepted.** Please refer to response to **a49.**		
a53. See recommendation **a8.**	**Management Response: Partially Accepted.** Please refer to response to **a8.**		
a55. See recommendation **a8.**	**Management Response: Partially Accepted.** Please refer to response to **a8.**		
a58. See recommendation **a8.**	**Management Response: Accept.** A full end to end review of the existing guidance on the handling of "solicitor's letters" will be undertaken - from the receipt and processing of the initial enquiry, to the release of information and supportive quality controls. C3 IR will work with Information Management to ensure a corporate approach with other force areas and that all aspects of this process are fully compliant with legislative guidance and SOP pertaining to		

	Information Sharing. Following the review - process guidance will be circulated to IR operators and formal copy retained within the Departmental shared drive for reference. In order to ensure that the process remains in line with the Guidance, we will set up a review schedule for the process, to match the review timelines of the SOPs. **Owner:** C3 **Implementation Date:** 14/02/2017		
a59. PSoS should seek to review best practice across the Command areas and implement a standard operational process for dealing with request from third parties / disclosure requests.	**Management Response: Accept.** Existing legacy force processes were set up in line with the legacy demand requirements and RTC data is received via Force Form 442 - which is an 8 page document. Guidance on what data can be released is based on the information contained within the form relating to non-injury and injury incidents. Note: if the enquiry is from a member of the public then personal info is redacted so that only name, insurance		

	details and the info relating to date/time locus of accident is shared. We acknowledge a variance across the legacy areas in how abstracts are processed across Scotland - these different processes have evolved according to the local data systems used and there are also variances in demand, staffing and historic local agreements. However despite these differences and the absence of a single national structure for this work - the data released still complies with relevant SOPS and legislative guidance. Also, we do consult with "regional" Information Management disclosure SPOCS if we receive any ad hoc enquires unrelated to the abstract process, in order to ensure that we remain compliant. The Abstract SOP is due for renewal and C3 will assist Information Management with that review when called upon to contribute. Whilst C3 can		

	contribute to a national review of the RTC Abstract process to identify best practice and establish a single corporate approach, it should be understood that IR has no authority or remit to impose change on a national basis. However, C3 will coordinate the formation of a short-life WG, made up of C3/IM/CJ/IR to move towards discharge or partial discharge pending future organisational change. **Owner:** C3 **Implementation Date:** 28/02/2017		
a61. A log designed to specifically record all the requests received should be created which captures the detail as to what personal data has been disclosed and the rationale as to why. Sample checking of disclosures should also be undertaken to ensure quality and consistency in disclosures being	**Management Response: Accept.** Specifically relating to the existing 442 RTC database - it is a local in-house system. There are limitations in the design of the database as it was not set up to manage the end-to-end abstract process and to record quality checking activity. When the mail arrives, all abstract and precognition requests are reviewed and		

made.	the operator will perform checks to ensure: • the legitimacy of the request • that payment is correct • the incident relates to our regional area • the query is sufficiently detailed to carry out a search Details released will pertain to whether the enquiry is from an insurance company/solicitor or from a member of the public. Guidance of what info is released is strictly applied. In addition, 100% Quality checking is undertaken on staff learning the process - and they are deemed to competent when the 95% quality mark has been consistently attained. Checking is undertaken by the team leader and quality sheets produced for operator feedback.		

	C3 IR is currently in talks with ICT to review our processes with a view to develop a new electronic procedure to manage RTC business and to enhance governance. **Owner:** C3 **Implementation Date:** ICT dependent		
a66. Sample checking of disclosures should also be undertaken to ensure quality and consistency in information being shared with the Local Area Commander for disclosure.	**Management Response: Partially Accept.** Please refer to the response to **a30.** As an organisation, work is ongoing to bring in quality assurance checks for divisions to assure quality at a local level and consistency at a national level. In addition, Local Policing will seek to work with divisions in terms of process and quality of product in anticipation of this being implemented. **Owner:** Chief Inspector Local Policing **Implementation Date:** 30/06/2017		
a67. See recommendation **a59.**	**Management Response: Partially Accepted.** The revised Information Sharing SOP, guidance and Intranet		

	information will support the development and use of standardised working practices where appropriate. Please also refer to the response to **a30**. **Owner:** Head of Information Management **Implementation Date:** 31/12/2017		
a70. The best practice operational model for the Concern Hubs should be implemented across all Divisions as soon as practicable. PSoS should also consider if any lessons learned or elements of the best practice model developed can be introduced into other data sharing activity.	**Management Response: Accepted.** The training schedule has been developed and will roll out during 2017. **Owner:** SCD **Implementation Date:** Starting December 2016		

I can confirm that this management response is a true representation of the current situation regarding progress made against our Action Plan outlined in the ICO Data Protection Audit Report dated 2 December 2016.

Signature……………..

Position………………..

Organisation……….