Part 3: Checklist with respect to any data sharing protocol

This checklist is extracted from my chapter on data sharing in "Data Protection for Financial Firms: A Practical Guide to Managing Privacy and Information Risk"; Edited by Tim Gough. Details on http://riskbooks.com/Operational%20Risk/data_protection_for_financial_firms.php

Obviously data sharing requires prior thought and the Information Commissioner has published a framework Code of Practice on Information Sharing. This part of this chapter amplifies this Code by providing a check list of issues that need to be covered. Of course, not ***all*** of the list below will be relevant to a specific data sharing protocol. Some of the checks might be best dealt with in documentation that is linked to a data sharing protocol. To reassure the public about data sharing, all relevant documentation should be in the public domain and where details are withheld (e.g. on security grounds), that this is identified publicly. Many of the issues (especially in Part 2 of this check-list) also apply to one-off requests for the disclosure of personal data.

1. **Does the data sharing protocol identify:**
    - Objectives of the data sharing and why sharing is necessary?
    - How the successes of all data sharing objectives are measured?
    - Reporting performance in terms of these objectives?
    - Senior managers identified as being responsible for implementation of the protocol?
    - Management commitment to implement, resource and review all data protection and security obligations?
    - Identification of all data controllers/third parties involved in the protocol?
    - The items of personal data covered in the data sharing?
    - The legal/statutory basis for the data sharing and any subsequent processing?
    - The complete list of purposes associated with data sharing?
    - The results of any Privacy Impact Assessment covering the proposed data sharing.
    - What happens to shared personal data if the protocol is ignored by a party to the protocol?
    - Conditions when a data controller joins or ceases to be subject to the protocol?
    - Conditions when a party to the data sharing agreement can be excluded from the protocol?
    - Links to other relevant policies (e.g. security, training, risk assessment)?
    - When common operating procedures applied to the protocol are reviewed?

2. **Does the data sharing protocol cover how the Data Protection Principles apply in the following areas:**

- Rules/authorisation procedures that permit further (onward) disclosure/data sharing?
- Rules/authorisation procedures that limits any further processing or data sharing?
- Contact points in relation to each party to the sharing agreement?
- How to obtain data subject consent to any data sharing if appropriate?
- Fair processing notices that contain a complete description of the data sharing?
- Procedure if public authorities not subject to the protocol **demand** access to shared personal data?
- Procedure if third parties not subject to the protocol **request** voluntary disclosure of shared personal data?
- How all parties to the protocol correct any inaccurate personal data that are discovered?
- Procedure if the content or accuracy of the personal data is challenged by data subjects?
- Common approach to subject access (especially when an access request is to personal data originating from another party to the protocol)?
- Dealing with the data subject's right to object to the data sharing?
- Application of any exemption to the right of access or from the non-disclosure provisions?
- Common retention criteria following data sharing?
- Expected standards adopted by each party in relation to the security of shared personal data?
- Reporting procedure if there is a significant breach of security (e.g. data loss)?
- Any special contingency requirements in case of interruption to the data sharing arrangements?
- Audit trail standards that reflect the nature of the sharing and who has had access to the shared personal data?
- Common notifications to the Information Commissioner that cover the data sharing?
- Restrictions on the transfer of personal data outside the European Economic Area without approval from parties to the protocol?
- Record keeping standards with respect to each of the above?
- Procedures to disseminate advice from the Information Commissioner (or any other regulator that has remit with respect to the processing of personal data).
- Procedures should there be enforcement action undertaken by the Information Commissioner (or any other regulator that has remit with respect to the processing of personal data).

3. **Does the data sharing protocol identify the commitments and expected management standards concerning:**

   - Staffing levels and the training staff in relevant procedures covering the above?
   - Whether temporary staff can have access shared personal data?
   - The use of agents to provide services that require access to shared personal data (e.g. data processors)?
   - How divergences in the level of protection are overcome if data sharing involves multiple data protection jurisdictions.
   - Standard contract terms covering data protection and security if data processors are used?
   - Regular review or audit of all protocol procedures and of record keeping to all parties of the protocol including staff, agents and data processors?
   - Improving and testing procedures, possibly based on penetration testing?
   - How to extend the protocol to include other parties?
   - Regular risk assessments to identify the risks associated with data sharing and relevant countermeasures; includes Privacy Impact Assessments?
   - Redrafting or refining the text of the protocol?
   - Dealing with problems raised by parties to the sharing agreement and by data subjects in relation to its operation?
   - If data sharing involves a public body, anticipation that information relating to data sharing protocol and related procedures may be subject to Freedom of Information requests?
   - A commitment to co-operate with the Information Commissioner in general and to be audited by the Information Commissioner if there is a problem?

4. **Is there evidence that <u>ALL</u> the above have been attended to?**

   Public authorities subject to a Freedom of Information regime should anticipate access requests to how the protocol operates in practice.

AMBERHAWK

PUTTING THE DATA PROTECTION INTO DATA SHARING

Amberhawk has developed courses focusing on all aspects of data sharing. These include training sessions for managers or staff tailored to your specific data sharing protocol or detailed legal training for your data protection officer.

For details e-mail info@amberhawk.com or visit www.amberhawk.com