Appendix to Section 5 - Data Integrity of the National Accreditation Standard

This document has been developed by Partners Against Business Crime in the Midlands to assist Business Crime Partnerships to understand the requirements of Section 5 - Data Integrity of the National Accreditation Standard and includes advice from the Information Commissioners Office on Data Security.

To ensure that sharing of data is fair and lawful, instances of sharing should be considered on a case by case basis and a clear justification of how such exchanges of data fulfil the requirements of the DPA recorded. In addition, where necessary, condition(s) for processing should be recorded.

The ICO has published an updated **PRIVACY IMPACT ASSESSMENT (PIA)** – privacy by design PIA Code of Practice**.** The code explains the privacy issues that organisations should consider when conducting a PIA.

Roles and Responsibilities

Make sure that you identify person/s for the security, seniority, reporting to the Board of Management/Data Controllers and that they fully understand their responsibilities giving commitment and direction from the top with a clear strategy, policy and assurance.

Physical Security

Provide adequate security of your premises to protect data including written policies physical security, entry controls, identification badges. Checks of deletion or destruction, shredding, waste disposal contractors, file storage and operating a clear desk policy. Mobile devices should be authorised for use and encrypted.

Identity Access Management

Setting up a new member on your scheme is easy but they will leave or move regularly so it is essential that processes are in place to ensure data is accurate and up to date. Have strong password controls and changes and wherever possible automated administration accounts set up as a default. Printing is done securely.

Training

Train your staff:

- so they know what is expected of them;
- to be wary of people who may try to trick them into giving out personal details;
- so that they can be prosecuted if they deliberately give out personal details without permission;
- to use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
- not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
- Provide appropriate training for key staff responsibilities for SAR disclosures, redactions or data sharing.

Computer security

- Install a firewall and virus-checking on your computers.

- Make sure that your operating system is set up to receive automatic updates.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allow your staff access to the information they need to do their job and don't let them share passwords.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don't lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

Email security

- Consider whether the content of the email should be encrypted or password protected. Your IT or security team should be able to assist you with encryption.
- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - e.g. "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.
- not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);
- not to open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service.

Fax security

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.
- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.
- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

Incident Reporting
Identify your incident reporting policy and provide training to users. The system you use should log system access. Any Data breaches to be notified to the Information Commissioner. Data subjects should be notified that you are storing their data and what you will do with it. Transparency of personal data use is essential.

Home Working
Home working has to be authorised with a well defined policy on use. Is this a one off authorisation or a regular occurrence? If this is a regular occurrence then it is recommended that physical and computer security measures must be put in place as described in Computer Security above. Equipment safeguards will include encryption, VPN, WPA2, security guidelines for manual records and disposal of personal data at home with regular compliance checks.

Collection of Data
Identify an individual with clear responsibility for records management issues who is experienced/qualified and who has sufficient authority to ensure organisational cooperation.

Information will be processed fairly in respect of data subjects when initially collected.

Maintenance of records
Steps are taken to ensure the quality of electronic and manual records: that are adequate, relevant, accurate, up to date and not excessive.

Indexing and Tracking of Records
Systems will be in place to record the location of records when active, in transit or archived.

Retention Schedules
Principle 5 of the Data Protection Act states that “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.”

You are required by the Lord Chancellor's Code of Practice on the Management of Records issued under Section 46 of the Freedom of Information Act 2000 to have and to implement a records retention and disposal schedule.
You should ensure that weeding, disposal and archiving of records is carried out in line with those schedules.

Disposal of Data
Are procedures in place for disposing of manual and electronic records with appropriate methods of destruction? Keep records of all data disposed of and that contracts are in place to cover the destruction and disposal of records by third parties.

Records Monitoring
Keep a log of requests received that records the receipt and processing of Subject Access Requests (SAR).

Accountability
Identify a key post, individual or team to be responsible for the management and or processing of requests for personal data.

Redactions/Exemptions

Data redaction is the suppression of sensitive **data**, such as any personally identifiable information (PII). PII can be used on its own or with other information to identify or locate a single person, or to identify an individual in context.
In such cases identify the legal basis for redaction and ensure checks are carried out keeping records of the legal basis for any exemption. That there is evidence of approval or quality assurance of applied exemptions.

Data Sharing

Where there is data sharing in place ensure there are protocols/agreements in place that are signed off and reviewed.

Author: David Wilson

MANSFIELDBID
Let's back Mansfield

December 2016