AMBERHAWK

ACCOUNTABILITY, UNDERTAKINGS AND AUDIT

NADPO: NOVEMBER 2011

chris.pounder@amberhawk.com
www.amberhawk.com

THE FUTURE IS ACCOUNTABILITY

ICO is stepping up the compliance checking and there is an Accountability Principle on the horizon.

Focus of the Principle is on management issues and records of the Controller's data protection compliance

The "Consensual Audit" and the "Undertaking" gives us a glimpse of the future.

MORAL: REVIEW QUALITY OF RECORDS OF ACTIVITY

ACCOUNTABILITY PRINCIPLE

- Principle already part of the OECD Guidelines ("A data controller should be accountable for complying with measures which give effect to the principles stated above")
- I think we have it already (7th Principle via "organisational measures" and S.4(1) – obligation to apply the Principles)
- DP "Principles and obligations are often insufficiently reflected in concrete internal measures and practices. Unless data protection becomes part of the shared values and practices of an organization, and responsibilities for it are expressly assigned, effective compliance will be at considerable risk, and data protection mishaps are likely to continue". (***Working Party Paper 173***).

ACCOUNTABILITY PRINCIPLE

- A principle on accountability would oblige "data controllers to put in place appropriate and effective measures to ensure that the principles and obligations ... are complied with and to demonstrate so to supervisory authorities upon request.
- Expect the "principle to impact other areas, including international data transfers, notification requirements, sanctions", and any future "certification programs or seals".

ICO's AUDIT ROLE

- An invitation for a "Consensual Audit" could follow a data loss or some other problem that has raised the Controller's profile.
- A statutory "spot check" audit in relation to Government Departments; can be extended to other public bodies but a Statutory Assessment Notice is subject to Appeal
- ICO agrees scope with you, the **staff to be interviewed** (i.e. YOU), the documentation to be reviewed, the personal data to be examined usually on-site (some data can be excluded).
- Three reports produced (draft, interim and final); executive summary usually in the public domain.

ICO's AUDIT ROLE

- Assessment Notices Code of Practice contains full detail
- Audit recommendations plus Red, Amber, Green; Amber split in two ("***Very limited assurance***","***Limited Assurance***", "***Reasonable Assurance***", "***High Assurance***")
- Remedial action plan documented and some details published
- Following an audit, enforcement action is unlikely but possible; Monetary Penalty Notice cannot be served

Plan for:

- Follow up audit by the ICO (e.g. North West London Hospitals NHS Trust**,** DEFRA, MOD, Law Society)
- Unresolved issues: what happens if the ICO audit team go "walkabout" into issues not in the agreed scope?
- FOI Requests pertaining to the audit or subsequent action

PUBLIC BODIES AUDITED

- Councils
  - Burnley Borough Council
  - Kirklees Neighbourhood Housing - ***LIMITED ASSURANCE***
  - Newcastle City Council - ***LIMITED ASSURANCE***
  - Portsmouth City Council
- NHS
  - Aneurin Bevan Health Board
  - Ayrshire and Arran NHS Scotland
  - North West London Hospitals NHS Trust
  - Papworth Hospital

PUBLIC BODIES AUDITED

- Police
  - Lancashire Police
  - Metropolitan Police
- Government Departments or Agencies
  - Crown Prosecution Service
  - DEFRA - ***GREEN***
  - DFPNI
  - Highways Agency
  - Ministry of Defence

PRIVATE BODIES AUDITED

Private sector

- GE Money Home Lending - ***GREEN***
- Google Inc
- Nationwide Building Society - ***GREEN***
- Trafford Housing : ***not published (impressions??)***

Other Institutions

- Royal Society - ***LIMITED ASSURANCE***
- Soldiers, Sailors, Airmen and Families Association (SSAFA) - ***LIMITED ASSURANCE***
- The Law Society - ***LIMITED ASSURANCE***

ICO's ASSESSMENT POLICY

ICO first looks at evidence in the controller's documentation:

- Strategies, Policies, Procedures
- Guidance and Codes of Practice
- Protocols, Frameworks & Memoranda of Understanding
- Training Materials
- Contracts (e.g. Data processor, employee)
- Privacy Statements (Fair processing notice)
- Privacy Impact Assessments
- Control Data
- Job Descriptions and Terms of Reference

Note: most of the above relate to management issues

ICO's ASSESSMENT POLICY

(Particular "red lines")

- Data Protection Governance: identify, implement and monitor the controls by which compliance can be measured and reported to management
- provide and monitor staff training and awareness regarding the correct use & management of personal data
- implement security measures which adequately protect personal data including on mobile and portable devices
- appropriately control and secure manual personal data both within and outside the 'data controllers' premises
- ensure Subject Access Requests are dealt with appropriately within the 40 day period

KIRKLEES HOUSING

(Arms length Housing Dept)

- No named Data Protection Officer. No clear accountability for DP compliance. Known weaknesses in DPA processes not yet addressed. No formal Information Asset Register or Information Asset Owners
- Optical drives and USB ports fully enabled; databases of personal data can be copied to USB memory devices or to DVD / CDs with ease.
- Unclear responsibility and ownership for data sharing lay at a corporate level. The frequency, type and nature of disclosures by KNH may increase the risks of inappropriate or excessive sharing with partners. Data sharing protocols examined were not always supported by current data sharing agreements or signed by an appropriately senior member of staff within each organisation. There was no evidence of independent corporate assessment or monitoring of existing data sharing agreements and protocols, for example, by Internal Audit.
- Staff demonstrated a limited awareness of required Data Protection and Information Security knowledge.

PORTSMOUTH COUNCIL AUDIT

- Policies do not consistently show the date of production, last review and owner of the document. Several documents had not been developed for a number of years.
- Inconsistencies between the ICT IG Strategy and the DP Code of Practice indicate a disjointed approach to data protection. No central oversight of data protection compliance level or control activity in the departments by any central committee or group. Very few statistics collected on PCC's compliance with the DPA 98.
- Information about subject access requests (SAR) and third party request are not collated corporately and used to provide PCC with an overview of their compliance although the IG team and Social Care collate their own data to measure some elements of compliance.
- Some recommendations from 2008 internal audit still outstanding. There is no central reporting or corporate requirement for departments to undertake PIA., no corporate overview of the training and no evidence of an Information Asset Register, either for electronic records or manual records.
- Retention schedules have not been adequately enforced in relation to electronic records that PCC are processing. Little corporate oversight or monitoring of the sharing of personal data.

THE UNDERTAKING

- Not a formal enforcement mechanism so no appeal
- Triggered by reported data loss or other event (usually a set of miffed data subjects)
- CEO of data controller promises to do better (e.g. implement 7th Principle; better training etc)
- Undertaking in the public domain with publicity
- Refusing to sign up might prompt formal enforcement
- Likely to be assessed later (e.g. via audit powers)
- Does not tie up ICO's resources like formal enforcement.
- Most linked to 7th Principle; but can apply to any Principle

COUNCIL UNDERTAKINGS

Eastleigh Borough Council. Potential disclosure sensitive personal data.

Dumfries and Galloway: Posting exempt details about staff on web-site following FOI request

Kirklees Metropolitan Council. Inappropriate disclosure of personal data by care workers contracted by Kirklees Metropolitan Council.

London Borough of Greenwich. Sensitive personal data was inadvertently disclosed; Council failed to implement ICT policy,

London Borough of Lewisham. Unencrypted USB stick containing thousands of tenant records and financial data in a London pub.

Luton Borough Council. Flawed encryption function in memory sticks.

North Lanarkshire Council. Theft of hard copy documents containing sensitive personal data.

Pool Borough Council. Faxes had been sent to the wrong number 3 times.

Somerset County Council. Social care records sent to the wrong family.

Walsall Council. Accidental disposal of personal data in skip by processor.

York City Council: individual's personal data, erroneously included with documentation sent to an unrelated third party.

NHS UNDERTAKINGS

- **Basildon and Thurrock University Hospitals NHS Foundation Trust:** fax containing sensitive personal data to the wrong recipient.
- **Birmingham East and North NHS Trust:** employees could access electronic files unrelated to the department they worked in.
- **Dartford and Gravesham NHS Trust: a**ccidental destruction of 10,000 archived records stored in a disposal room due to lack of space.
- **Dunelm Medical Practice:** fax transmission to wring number disclosed two patient's electronic discharge letters,
- **East Midlands Ambulance Service NHS Trust**. Fax to the wrong recipient.
- **London Ambulance Service NHS Trust**. Theft of unencrypted laptop.
- **Eastern and Coastal Kent Primary Care Trust**. Loss of a CD containing personal data during a move of office premises.
- **Ipswich Hospital NHS Trust.** 29 patient records found in a public place.
- **Lancashire Teaching Hospitals NHS Foundation Trust**. Fax to the wrong recipient on more than one occasion.

NHS UNDERTAKINGS

- **Liverpool Community Health NHS**: losing papers relating to the medical history of 31 children and their birth mothers during a premises move
- **Northamptonshire Healthcare NHS Foundation Trust**. Loss of one individual's medical records.
- **Poole Hospital NHS Foundation Trust:** two diaries containing details of 240 midwifery patients stolen from a nurse's car.
- **Royal Cornwall Hospitals NHS Trust**. Inappropriate disclosure of third party sensitive personal data on two occasions, in response to a SAR
- **Royal Liverpool & Broadgreen University Hospitals NHS Trust**. Two separate incidents involving the loss of personal data by the Trust.
- **UCL Hospitals NHS Foundation Trust**. Unencrypted memory stick found off Trust premises relating to 750 Trust patients.
- **University Hospital of South Manchester NHS Trust**. Loss of an unencrypted memory stick relating to 87 patients.
- **Warrington and Halton Hospitals NHS Foundation Trust**. Theft on an unencrypted laptop relating to 110 patients.

PRIVATE SECTOR

- **Co-operative Life Planning Limited:** Inappropriate disclosure of an electronic file containing many customer's personal data.
- **Internet Eyes Limited**. CCTV clip posted on video sharing website YouTube that contained an identifiable image of a person in a shop.
- **HCA International Limited**. Theft of two unencrypted laptops containing sensitive personal data from one of the group's hospitals.
- **Lush Cosmetics Ltd.** Malicious intrusion on their website which compromised approximately 5000 customer credit cards.
- **Raisa Saley, Barrister at law,** loss of a bundle of court papers which contained sensitive personal data relating to a number of individuals from the same family.

VOLUNTARY GROUPS

- **Asperger's Children & Carers Together** Theft of an unencrypted laptop containing sensitive personal data
- **Bay House School** : personal details of 20,000 individuals (7600 pupils) put at risk during a hacking attack on its website.
- **Holly Park School** - theft of an unencrypted laptop containing personal data relating to nine pupils.
- **Freehold Community School**. Theft of an unencrypted laptop and paperwork relating to 90 pupils from a teacher's car.
- **Cherubs Community Playgroup**. theft of an unencrypted laptop relating to 47 families.
- **Surbiton Children's Centre Nursery**. Theft of a teacher's bag containing an unencrypted memory stick and paperwork.
- **Wheelbase Motor Project**. Theft of an unencrypted portable hard drive storing sensitive personal data concerning 50 individuals.

OTHER

- **Association of School and College Leaders** (ASCL) - theft of a unecrypted laptop containing sensitive personal data from the home of an employee.
- **Norwich City College of Further and Higher Education**: two instances of inappropriate disposal of 80 student files, some of which contained sensitive personal data
- **Wandle Housing Association**. Unencrypted USB stick found in a London pub (thousands of tenant records and financial data)
- **Council for Healthcare Regulatory Excellence** (CHRE). Possible loss of sensitive personal data in complaint review files
- **Scottish Children's Reporter Administration.** Email containing sensitive personal data relating to a child's court hearing sent to an unknown third party; temporary loss of 9 case files relating to the safety and welfare of children during an office move.

UNDERTAKINGS GOVERNMENT?

- None
- Do you believe that?
- Only one is IPS in February 2011 for losing the passport renewal applications of 21 individuals.

FOI UNDERTAKINGS

For example:

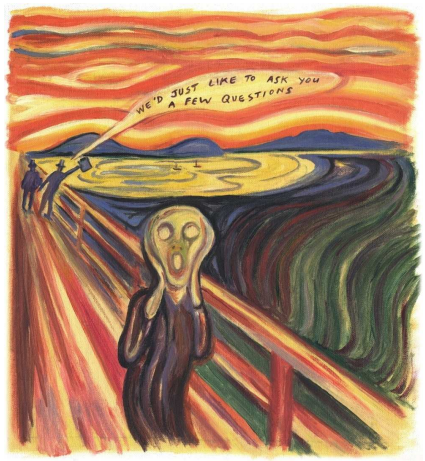
Westminster – FOI Undertaking

Islington – FOI Undertaking

Hammersmith & Fulham – FOI Undertaking

A new development!

THE END



Balanced Blog "Hawktalk"

and

Courses from Amberhawk Training Ltd

chris.pounder@amberhawk.com