
13 June 2012

View the Replay
Today’s Agenda


• Undertaking and enforcement of the ICO
• Security issues and responsibility involved with data sharing
• How to improve compliance with Data Protection
• Importance of Privacy Impact Assessments in changing environments
• ICO enforcement notices and civil monetary penalties
• Importance of audit logs for fundamental privacy and security in healthcare
• Q&A Session
Today’s Panel

Dawn Monaghan
Strategic Liaison Group Manager
Public Services
Information Commissioners Office
www.ico.gov.uk

Kurt J. Long
FairWarning® Founder and CEO
Kurt@FairWarning.com
727.576.6700  x101
Data Protection
Planning ahead, Who, What, Why and How
Possible consequences of a breach

Dawn Monaghan, Group Manager, Strategic Liaison ICO UK
An Enabler not a Barrier!

- It is important that the Data Protection Act is not perceived as an obstruction to change, data sharing or other business process.
- The aim of the legislation is to allow data to be processed and shared without risk to privacy.
- The key therefore is where possible to consider any Information governance impacts of new procedures, processes and systems when they are first conceived.
- Identify the risks and associated impacts to mitigate and manage those risks.
Key Considerations

- Think of personal data as an asset
- Information governance as a business process
- The proportionality of privacy versus transparency
- Have champions at every level of the organisation from board level across and down
- Ensure you have policies, systems, procedures and processes in place which are appropriate to the data you process/share
- More importantly train staff to not only have an awareness but understand your organisations and their individual responsibilities when handling personal data
What

- Personal data do you process?
- Collect
- Hold
- Use
- Share
- Retain

- Is it sensitive personal data
Why

- Are you processing the personal data?
  - Do you need to/still need to process it?
- Why are you sharing it with others?
  - Do you need to/still need to?
- Why are you receiving personal data from others?
  - Do you need to/still need to receive it?
- Why are you retaining the data?
How

- Are you collecting the data?
- Storing the data?
- Sharing the data?
- Is the data electronic/ hard copy/ both?
- Are you using it?
- Are you managing its accuracy?
- Are you storing it?
- Are you decommissioning it?
Who

- Knows you have the data?
- Do they know you have it and what you are using it for?
- Who has access to the data?
- Who has responsibility for the data?
- Data controller/ data processor
- Data controller in common or joint
- At organisational level
- Takes responsibility as the accountable officer
Accuracy

• Processes to ensure accuracy
• Monitoring to ensure processes
• Retention/disposal schedules
• Have you shared the data, have changes been made across the system?
• Harm if inaccurate?
Security

- ‘Technical and organisational measures’
- Outsourcing – are you confident?
- Following principle 7
- Written Contract
- Data sharing agreement
- Data Sharing code
Security

- Unauthorised or unlawful processing
- Do you know who has access to the data?
- Have they been properly trained?
- Do they fully understand what they can and can’t do with it?
- Do they understand what could happen if they misuse the data?
- Do you monitor the use of the data?
- Do you have procedures in place if the data is misused?
Planning Ahead – Privacy by design

- Eliminating the unexpected is difficult - Human error will always be present

- By planning you can at least eliminate the possibly expected – naive incompetence can often be avoided

- Use Privacy Impact Assessments to determine the likely risks and to assist in considering the mitigations
What happens if it goes wrong?

- Make sure you know ASAP
- Initiate procedures for damage limitations
- Presently the Act does not require breaches to be reported to the ICO
- In the UK the Department for Health requires NHS bodies to report breaches to them and to the ICO
- Many other organisations do report breaches to the ICO on a voluntary basis
- Advice as to what to do, preliminary investigation to determine the facts and the impacts of the breach.
- In many cases no further action taken
Undertakings

- Issue an undertaking on the organisation

- They commit an organisation to a particular course of action in order to improve its compliance

- Signed by the Chief Executive or equivalent to commit to action/s

- Binding, no end date

- Can be monitored/audited for compliance with undertaking
Enforcement Notices

- Serve an enforcement notice
- ‘Stop now’ order where there has been a breach
- Requires the organisation to take or refrain from taking specified steps in order to ensure they comply with the law
Civil Monetary Penalties

• Issue Civil Monetary Penalty notices requiring organisations to pay up to £500,000 for serious breaches of the Act which occurred on or after 6\textsuperscript{th} April 2010

• Applies to all data controllers in public, private and voluntary sectors

• Serious contravention of the Act by the data controller
Civil Monetary Penalties

- Breach likely to cause substantial damage or distress and either
  - Breach was deliberate or
  - Data controller knew or ought to have known a breach would occur and
  - The contravention would likely be substantial
  - The data controller failed to take reasonable steps to mitigate a breach
Avoiding a Breach

- Understand the organisation’s obligations
- Take it seriously
- Ensure all staff are aware of their responsibilities and the organisation’s policies and procedures and that they follow them
- At any point in time know what you have, why you have it, what you are doing with it and who is responsible for it.
- Think – Privacy by design
- Use the Privacy Impact assessment guidance
- Use the Data Sharing Code of Practice
- Access advice, guidance and assistance if required
Keep in touch

Subscribe to our e-newsletter at www.ico.gov.uk or find us on...

facebook

twitter

www.twitter.com/iconews

YouTube

LinkedIn

13 June 2012

FairWarning®
Trust but verify®
Patient Privacy Monitoring & Breach Detection

Consolidating and analyzing audit logs and other data from EHRs and healthcare applications for proactive patient privacy monitoring
Patient Privacy Monitoring & Breach Detection

- Full featured turn-key solution
  - Patient and user investigations
  - Proactive alerting with filtering
  - Ad hoc reporting
  - Incident tracking and reporting
  - Zero FTE system operation requirement
  - Remediation expertise or training is required

- 170+ Production supported EHRs and healthcare applications
- Affordable support – high touch 1-cost model
- Proven deployment methodology and documentation
Audit logs mandatory for privacy & security fundamentals

✓ Audit logs mandatory for forensics investigations involving patients & users
✓ Audit logs mandatory for proactive breach detection
✓ Audit logs required for fulfillment of IGT
✓ Audit logs required for patient disclosure reports
✓ Insist your electronic health record vendor enables audit logging
✓ Insist audit logs are protected and unalterable
✓ Insist all applications that access patient health information produce audit logs

For more information on FairWarning® Ready, email solutions@FairWarning.com
Questions & Answers

Q: In regard to accuracy, are there any suggested templates or metrics for checking accuracy?
A: There are no templates as such, but many organisations have a process for sending a ‘check’ form to individuals on a regular basis so that they can confirm ‘no change’ to their details or can submit new information. Some organisations’ websites allow you to change your details whenever you need to, and remind individuals at ‘log in’ or ‘log out’ to do this.

Q: There is currently no incentive for a private data controller to voluntarily report breaches to the ICO if not mandated to, especially seeing monetary penalties being imposed. Are there any moves to alter this?
A: No, there are no plans to change this. The Act does not dictate voluntary reporting and neither does the ICO. It is in the interests of a controller to report a breach though, firstly because they can, then to be assured they have done everything possible to contain the breach and/or mitigate it from happening in the future.

Q: What is best way to measure or assess accuracy? Any templates or suggested approaches? A: See answer 1
Q: Will PIA be mandatory or are they/will they remain voluntary?
A: They will remain voluntary as long as the Law doesn’t require them. Presently they are a ‘good practice’ tool suggested by the UK ICO. However, it has been proposed by some that they should be mandatory in the new European Directive; if that happens then they may be made mandatory in the UK but that wouldn’t be for some time.

Q: How will ICO approach SIRO issues for local government? NHS has this already but local government is new to it. Any guidance from ICO?
A: The ICO are advocating to Local Government that they have a system that facilitates meeting obligations of the Act. Having a SIRO is one way of achieving that, always assuming that the SIRO understands and can deliver the responsibilities of the role. Local Government generally does have an ‘accountable Officer’ although they are not termed SIRO.

It may be helpful in the future, particularly for the interface between Health and public health for a consistent title to be given to the ‘accountable person’ but it is for the organisations to decide who this should be not the ICO.
Today’s Panel

Dawn Monaghan
Strategic Liaison Group Manager
Public Services
Information Commissioners Office
www.ico.gov.uk

Kurt J. Long
FairWarning® Founder and CEO
Kurt@FairWarning.com
727.576.6700 x101