

# 2011 Executive Webinar Series

The State of Enforcement:  
Protecting Patient Privacy and  
Complying with the  
Data Protection Act

[View the Full Replay](#)

# FAIRWARNING®

*Trust but verify®*



# Today's Agenda



- Introduction
- Mick Gorrill, Head of Enforcement, Information Commissioner's Office
- Kurt Long, FairWarning®
- Hazel Grant, Partner, Bristow's
- Questions & Answers

FAIRWARNING®

*Trust but verify*®



**MICK GORRILL, HEAD OF ENFORCEMENT  
INFORMATION COMMISSIONER'S OFFICE**

# The Information Commissioner: Enforcement and Investigations.

Mick Gorrill

Head of Enforcement.

**ico.**

Information Commissioner's Office

# New structure

- Enforcement Division
- Responsibility for Data Protection Act and Freedom of Information Act
- Bigger enforcement teams
- Concentration on serious breaches of the DPA and FOIA
- Audit which was a part of the RAD now becomes part of the new Good Practice Department.

# New structure

Also responsible for the investigation of three criminal offences:

Section 55 Data Protection Act,

Section 17 Data Protection Act,

Section 77 Freedom of Information Act.

# Civil Monetary Penalties.

Background,

Policy objectives,

Legislative framework,

Main features,

Specific requirements.

# Background

- Significant losses of personal data in 2007
- Existing powers deemed inadequate
- Public calls for criminal offence
- Preferred option was power to impose a Monetary Penalty – civil sanction
- New power inserted into section 55 of Data Protection Act 1998 by section 144 of the Criminal Justice and Immigration Act 2008 (CJIA)

# Policy objectives

- Enhanced power for ICO to impose monetary penalties
- Sanction and a deterrent to data controllers who may otherwise ignore their responsibilities under the Data Protection Act
- Encourage data controllers to approach ICO and promote compliance
- Improve public confidence

# Civil Monetary Penalties.

To date four monetary penalties have been issued all of which involve breaches of the 7<sup>th</sup> data protection principle.

7<sup>th</sup> principle:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

# Section 55 DPA 1998.

It is an offence for a person, knowingly or recklessly, without the consent of the data controller, to:

obtain or disclose personal data or the information contained in personal data;

or

procure the disclosure to another person of the information contained in personal data

# Section 55 DPA 1998.

If a person has obtained personal data in contravention of section 55(1) it is an offence to sell or offer to sell personal data.

ICO receive around 200 allegations of Section 55 every year.

Around 50 or so go forward for investigation.

# Section 55 DPA 1998.

It is the view of the ICO that viewing personal information held digitally may amount to unlawful obtaining –

For example, where individuals are told they may only view the recorded information of persons whom they are dealing with and decide to look at other records out of curiosity.

# Strategic regulator.

Being a strategic regulator means that, in so far as we have a choice, we have to be selective with our interventions.

We will therefore apply our limited resources in ways that deliver the maximum return in terms of a sustained reduction in data protection risk.

That is the risk of harm through improper use of personal information –

# Section 55 DPA 1998

Main criteria when assessing allegations of S55 is the harm or distress caused to the data subject,

normally,

business to business IFA, hairdressers etc, no detriment,

curiosity – dealt with by internal discipline,

domestic issues – where the information is used – potentially prosecution or caution.

# Section 55 DPA 1998

Nurse and husband split up

His new partner was pregnant and would have to attend the maternity dept.

Nurse accessed patient information to check up on the status of the “competition”

Cautioned

# Section 55 DPA 1998

Call centre staff member takes a call from a female customer

Decides he likes the sound of her so obtains her number from the system

Texts her in an attempt to start a romantic liaison

Disciplined and sacked.

Cautioned for S55 offence.

# Section 55 DPA 1998

Where personal information has been unlawfully obtained and later sold or used in a manner calculated to cause harm or distress to a data subject the ICO will always investigate and seek to prosecute those responsible,

for example,

personal information unlawfully obtained by a private investigator and sold on ( financial gain )

personal information unlawfully obtained and used to embarrass or cause distress – medical record.

# Section 55 DPA 1998

Personal information relating to patients in hospital sold onto claims organisations ( financial gain)

Persons unlawfully accessing by pretext public and private sector organisations to obtain information about individuals to trace their whereabouts and profile any income,

Where a prosecution is in the public interest – unlawful obtaining may become prevalent.

Unlawful obtaining a precursor to a criminal offence ( Police).

# Section 55 DPA 1998

Reputational damage to organisation when staff access personal data unlawfully,

If widespread there is a possibility that the data controller/organisation may be subject to a civil monetary penalty.

# Avoiding Penalties and ensuring compliance

Any Questions?

FAIRWARNING®

*Trust but verify*®



KURT LONG, FOUNDER

FAIRWARNING®

# Breach detection, compliance, governance, security

- ❑ Dramatically reduce risks associated with privacy breaches. Privacy breach = “inappropriate use of access to electronic health records”
- ❑ Full featured turn-key solution
  - ❑ Breach definition & consequences - Investigation, monitoring, alerting, remediating and governance reporting
  - ❑ Deters snooping, medical identity theft, identity theft
  - ❑ Risk Assessment and associated gaps
- ❑ Alert on 200+ patient privacy analytics with filtering
- ❑ 100+ EHRs and healthcare applications supported out-of-the-box
- ❑ Comprehensive rollout documentation – Data Definition Guides & Implementation Toolkit
- ❑ Affordable support – high touch 1-cost model
- ❑ Over 100 customers in production or on way, massive scale, KLAS coverage

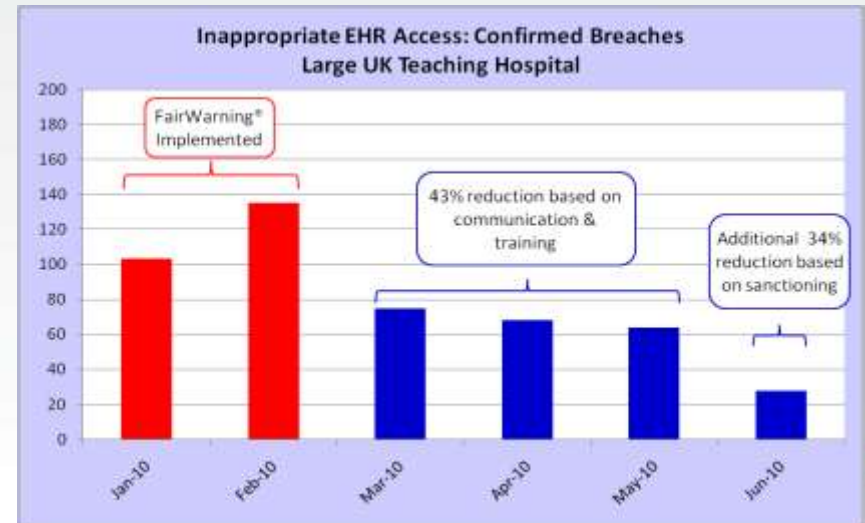
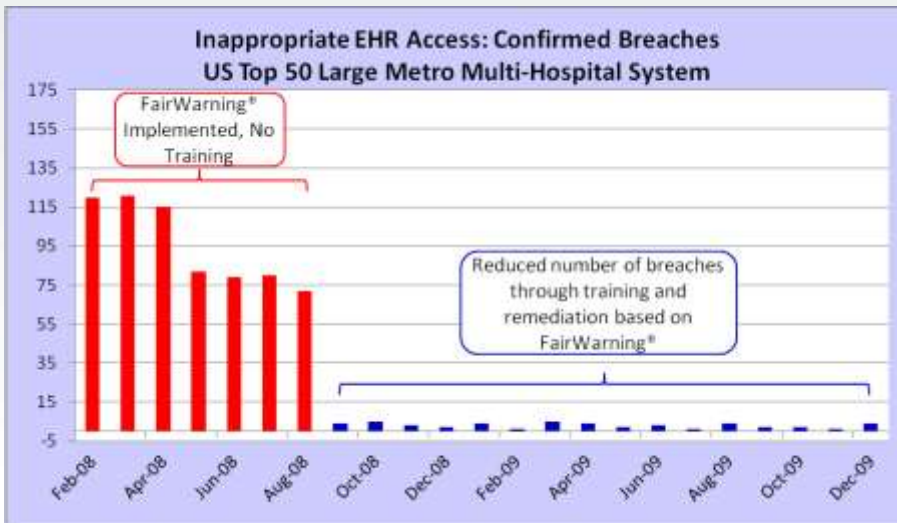
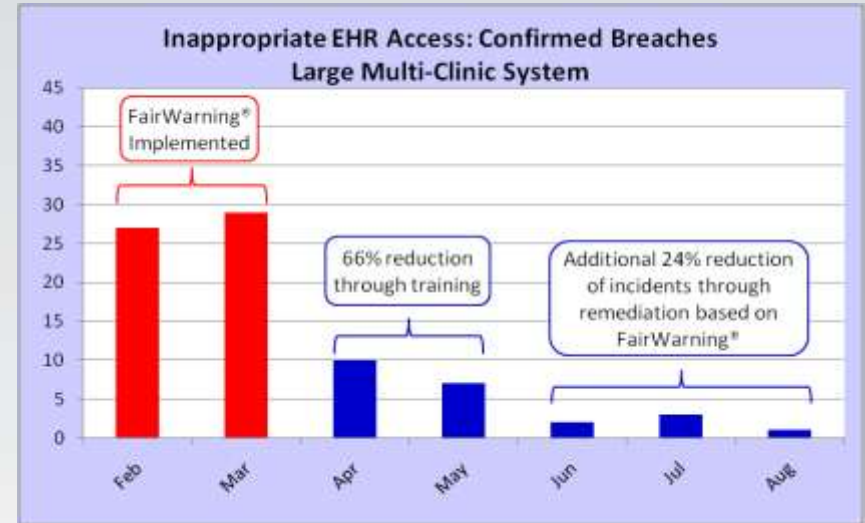
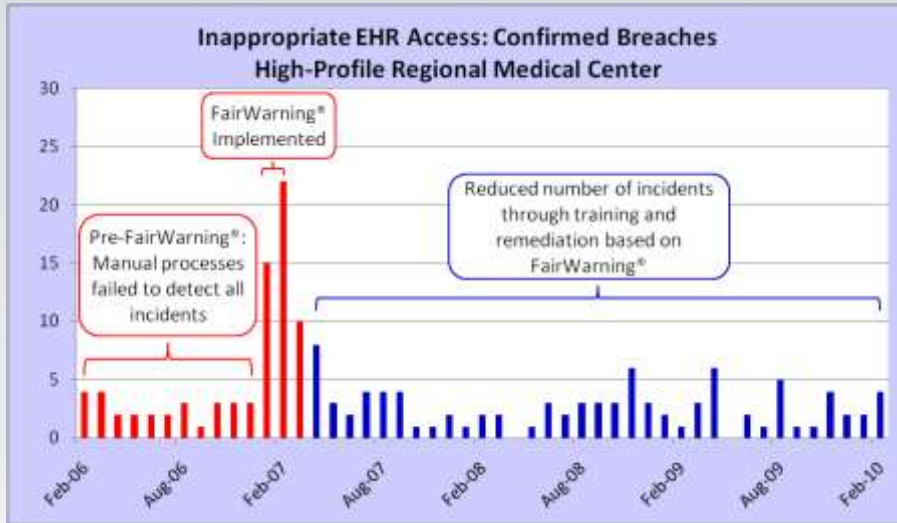


# FairWarning® Customer Community



- 100 + major enterprise healthcare providers, 18 new in Q4 2010 alone
- Represent 450 hospitals and 2,100 clinics
- United States, Canada, United Kingdom
- 50 % + have received prestigious awards for quality
- Range in size from 1,000 to 50,000 + employees
- Note: FairWarning® now has offices in London, England and Paris, France

# Breach monitoring creates a “Culture of Privacy & Compliance”



# FairWarning<sup>®</sup> and Compliance

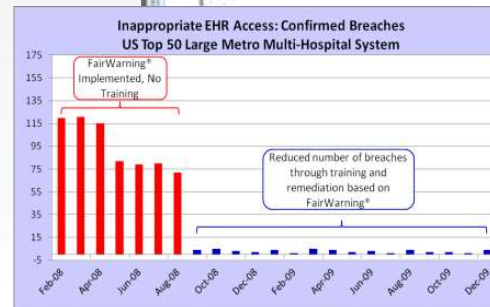
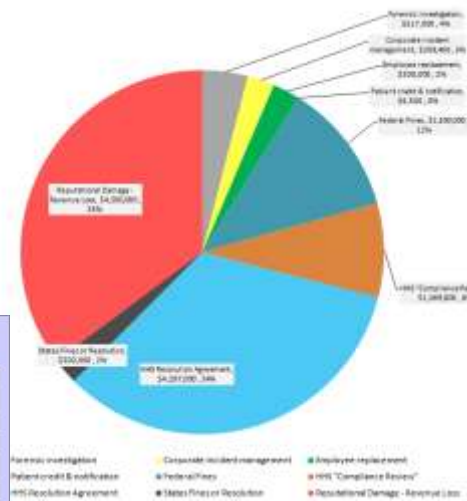
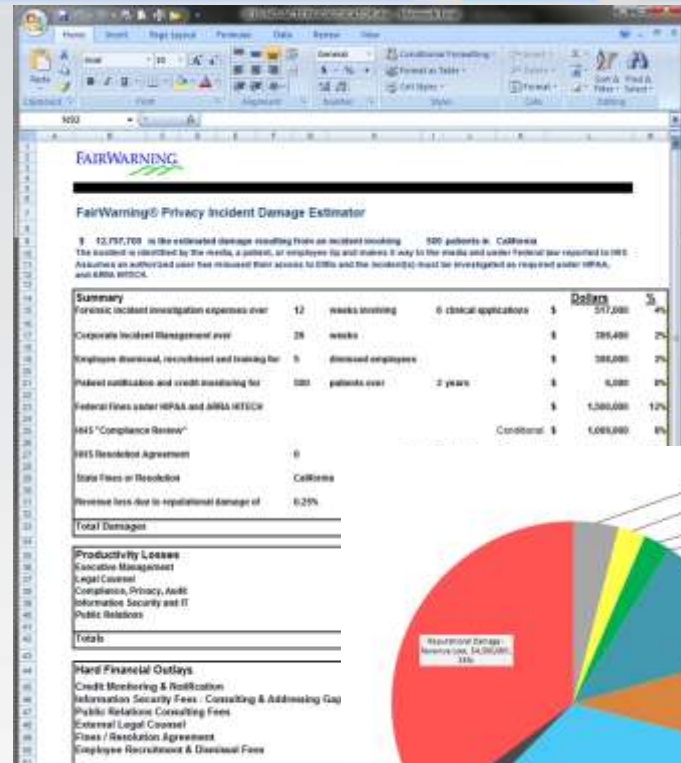
FairWarning <sup>®</sup> Features	Data Protection Act 1998	Computer Misuse Act 1990	NHS Information Governance Toolkit (IGT)	NHS Confidentiality Code of Practice	Additional Regulations
<ul style="list-style-type: none"> <li>• <i>Automatic Patient Privacy Alerts and email notification</i></li> <li>• <i>100+ patient privacy behavior-based analytics</i></li> <li>• <i>Privacy Alerts Tracking, Trending, Reporting</i></li> </ul>	<p><b>REQUIREMENT. Data Protection Principle #1:</b> Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless the processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.</p> <p><b>REQUIREMENT. Data Protection Principle #7:</b> Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.</p>	<p><b>REQUIREMENT. Make provision for securing computer material against unauthorised access or modification.</b> Unlawful access is committed if the individual intentionally gains access; knowing he is not entitled to do so; and aware he does not have consent to gain access.</p>	<p><b>REQUIREMENT. 8-206:</b> Monitor and audit access to confidential person information.</p> <p><b>REQUIREMENT. 8-305:</b> Regular reviews are carried out to audit and assure the access control and management processes.</p>	<p><b>REQUIREMENT. Systems and processes that will restrict the use and disclosure of confidential patient information.</b></p> <p><b>REQUIREMENT. Access controls and authentication procedures.</b></p>	<p>Caldicott Guardian Manual 2006: Access should be on a strict need-to-know basis.</p> <p>Human Rights Act 1998</p>
<ul style="list-style-type: none"> <li>• <i>Governance &amp; Risk Analysis Reporting</i></li> </ul>			<p><b>REQUIREMENT. 8-302:</b> There are documented information security incident / event reporting and management procedures.</p> <p><b>REQUIREMENT. 8-302:</b> Monitor compliance with the security event reporting procedures.</p>		
<ul style="list-style-type: none"> <li>• <i>Patient Accounting of Disclosures across clinical applications</i></li> </ul>	<p><b>REQUIREMENT. Respond to subject access requests.</b> Must provide the requested information, as well as a list of people to whom you may disclose the information, and an explanation of why you may do so.</p>		<p><b>REQUIREMENT. 8-205:</b> Respond to individuals' requests for access to their personal data.</p>		
<ul style="list-style-type: none"> <li>• <i>Global incident investigation across clinical applications</i></li> <li>• <i>Saved "ad hoc" reporting</i></li> <li>• <i>Forensically sound repository</i></li> </ul>			<p><b>REQUIREMENT. 8-206:</b> Procedures for investigating confidentiality events.</p>		<p>Freedom of Information Act 2000: General right of access to information held by public authorities.</p>
<ul style="list-style-type: none"> <li>• <i>Results used with sanctioning and training</i></li> </ul>			<p><b>REQUIREMENT. 8-206:</b> Staff members have been made aware of the monitoring and auditing of access, the need for compliance, and sanctions for failure to comply.</p> <p><b>REQUIREMENT. 8-302:</b> Instigate remedial action where procedures have not been followed.</p>		<p>Caldicott Guardian Manual 2006: Everyone must understand his or her responsibilities.</p>

# FairWarning® Resources

Available after today's webinar:

- ❑ Patient Privacy Framework Guides
- ❑ ROI Calculator on privacy monitoring
- ❑ Breach Damages Estimator
  - ❑ Based on breach monitoring deployments as well as interviews with health systems, legal counsel and 3<sup>rd</sup>-parties involved with high-profile breaches and audits
- ❑ White paper on privacy breach findings

Both available by emailing  
[Solutions@FairwarningAudit.com](mailto:Solutions@FairwarningAudit.com)



**FAIRWARNING<sup>®</sup>**

*Trust but verify<sup>®</sup>*



**HAZEL GRANT, PARTNER  
BRISTOWS LAW FIRM**

BRISTOWS

---

# Employee Monitoring and Data Protection Compliance

23 February 2011

Hazel Grant, Partner



## Agenda

- Why monitor?
- What is monitoring?
- Legal and regulatory framework
- How to monitor?
- Risks of enforcement
- Key actions

# Why monitor your employees?

- Time-wasting
- Breach of data protection principles of fair and lawful use and data security
- Disclosure of confidential information
- Damage to corporate reputation
- Vicarious liability for discrimination claims
- Copyright infringement
- Defamation
- Theft
- Assess performance

# What is monitoring?

- Monitoring of email content and traffic
- Interception of telephone calls
- Monitoring of internet use
- CCTV
- In-vehicle monitoring
- Covert filming / recording
- Use of detectives
- Searching
- Review of social networking sites

# Legal and regulatory framework

- Human Rights Act 1998 and European Convention on Human Rights
- Data Protection Act 1998 [Directive 95/46/EC]
  - Part 3 of the Employment Practices Data Protection Code and Supplementary Guidance
- Regulation of Investigatory Powers Act 2000
  - Lawful Business Practice Regulations 2000
- Duty of trust and confidence implied into employment contracts and concept of fairness in employment law for disciplinary actions

# Legal and regulatory framework: Human Rights

- Only expressly applies to public authorities, but indirect impact through courts and employment tribunals
- ECHR – right to privacy in the workplace. But concept of ‘proportionality’ and permitted derogations
  - Article 8(1) right to respect for private and family life and correspondence
- Right to freedom of expression
  - Article 10(1) includes freedom to hold opinions and to receive and impart information and ideas
  - Article 10(2) subject to such conditions or restrictions as are prescribed by law and necessary...for the protection of the reputation or rights of others, for preventing disclosure of information received in confidence

# Legal and regulatory framework: Data Protection

- Data Protection Act 1998 – monitoring will involve the processing of personal data, therefore must comply with data protection principles
  - Fair processing notice
  - Processing conditions
    - Legitimate interests
    - Consent
    - Sensitive personal data
- Employment Practices Code – contains recommendations for monitoring in compliance with the DPA, so that any adverse impact on workers should be justified by the benefits to the employer

# Legal and regulatory framework: RIPA

- RIPA – Unlawful to intercept a communication in the course of transmission, but no interception:
  - if you record a call that you are listening to
  - when reviewing open emails or sent emails (generally accepted view)
- Criminal offence: unlawful interception on a private telecommunications system without the consent of the system owner
- Monitoring is lawful under RIPA:
  - with consent – if reasonable grounds for believing both sender and recipient have consented (NB – UK law under review)
  - without consent – on private networks with the consent of the system owner, through the Lawful Business Practice Regulations – provided for business purposes and all reasonable efforts made to inform users

# How to monitor? (1)

- Notification and awareness
  - Workers should be aware of the nature, extent and reasons for monitoring
  - Where practicable, those communicating with workers should be made aware of any monitoring and the purposes behind it
  - Workers should be aware through IT / electronic communications acceptable use policies what behaviour is and is not acceptable (and the consequences of a breach of the policy – disciplinary action / dismissal)
  - Workers should receive adequate training, reminder emails, pop-up on log on screen etc and check understanding
  - Acceptable use policy should cross-refer to other relevant policies, such as disciplinary and anti-harassment / equal opportunities policies

# How to monitor? (2)

- Impact Assessment
  - Identify purpose of monitoring and specific benefits to be obtained
  - Identify any likely adverse effect on workers
  - Consider alternatives to monitoring or less intrusive means (eg automated monitoring)
  - Covert monitoring can rarely be justified
  - Take into account steps taken to ensure compliance with laws (such as notifying workers or limiting access to data) and expectations of privacy
  - Determine (and document) whether the monitoring is justified

# How to monitor? (3)

- Authorisation at an appropriately senior level for every instance of monitoring (and ensure such persons are properly educated / advised)
- Ensure data is kept secure and only seen by those with a 'need to know'.
  - Monitoring should be carried out by appropriately trained staff – line managers may not be the most appropriate
- Avoid collecting excessive information and only use information for the purpose it was collected, unless it cannot reasonably be ignored
- Workers should have the opportunity to see the results and make representations

# Risk of ICO Enforcement (1)

- Fines for serious breaches causing substantial damage or distress which are deliberate or reckless and with no reasonable steps taken to prevent
- Process:
  - Step 1 – notice of intent
  - Step 2 (optional!) – written representations from controller – 21 days time limit
  - Step 3 – issue of fine notice
  - Step 4 (optional!)– right of appeal to first tier tribunal

# Risk of ICO Enforcement (2)

- A4e £60,000 fine, November 2010.
- Key factors?
  - ICO issued guidance on encryption of laptops containing personal data (Nov 2007)....failure to follow ICO guidance
  - Blamed home worker for not following IT policy....but should not have issued laptop unencrypted
  - In some cases, highly sensitive information and large number affected
  - Complaints/interest from affected individuals

# Risk of ICO Enforcement (3)

- Lessons to be learnt:
  - Do not assume that having the policy is enough
  - Prepare written representations, based on ICO publications e.g. ICO data protection and enforcement strategies
  - Do not ignore ICO guidance on e.g. encryption

# Key Actions

- **Know your risks and exposure**
  - carry out impact assessments for monitoring, carry out DP compliance audit more generally: *“this is your insurance policy”*
- **Keep an organised record of:**
  - policies, notices, consents, impact assessments, data protection compliance structure, your DP compliance record (e.g. staff training carried out, staff monitoring, contractor audits)
- **Have the right people in place**
  - data protection officer, reporting lines and responsibilities
- **Trying to be compliant is better than ignoring risks**
  - document your evaluations/decisions, show your goodwill



Thank you for your attention

Bristows

100 Victoria Embankment

London EC4Y 0DH

T +44(0)20 7400 8000

F +44(0)20 7400 8050

[hazel.grant@bristows.com](mailto:hazel.grant@bristows.com)

[www.bristows.com](http://www.bristows.com)

BRISTOWS

# FAIRWARNING®

*Trust but verify®*



## QUESTIONS & ANSWERS