

# FairWarning® 2010



making IT work

## Privacy & Security in the NHS: How Leading Organisations are Protecting Patient Privacy

July 20, 2010

[Please Click Here to View The Replay](#)

# FAIRWARNING®

*Trust but verify®*



# Today's Agenda



- Overview
- Northgate / NHS Lothian Case Study
- FairWarning® Product Demonstration
- Questions & Answers

# Patient privacy in EHRs



- Deployment of electronic health records growing
- Access by growing number of healthcare personnel
- Difficult to limit access control at granular level
- Pressure to exchange electronic records means even greater access
- Manual auditing processes impossible to sustain
- No proactive detection of EHR privacy breaches means only detect through patient incident or headlines

# NHS IGT 8-206: There are appropriate confidentiality audit procedures to monitor access to confidential personal information



**Description:** Organisations should ensure that access to confidential personal information is monitored and audited locally and in particular ensure that there are agreed procedures for investigating confidentiality events.

0: Insufficient evidence to attain Level 1

- 1: **DOCUMENT:** There are documented confidentiality audit procedures in place that include the assignment of responsibility for monitoring and auditing access to confidential personal information. The procedures have been approved by senior management or committee and have been made available throughout the organisation
- 2: **EDUCATE & IMPLEMENT:** All staff members with the potential to access confidential personal information have been made aware of the procedures. The procedures have been implemented and appropriate action is taken where confidentiality processes have been breached.
- 3: **AUTOMATE & TRAIN.** Access to confidential personal information is regularly reviewed. Where necessary, measures are put in place to reduce or eliminate frequently encountered confidentiality events.

Please see <https://www.igt.connectingforhealth.nhs.uk> for more information

# Breach detection, compliance, governance, security

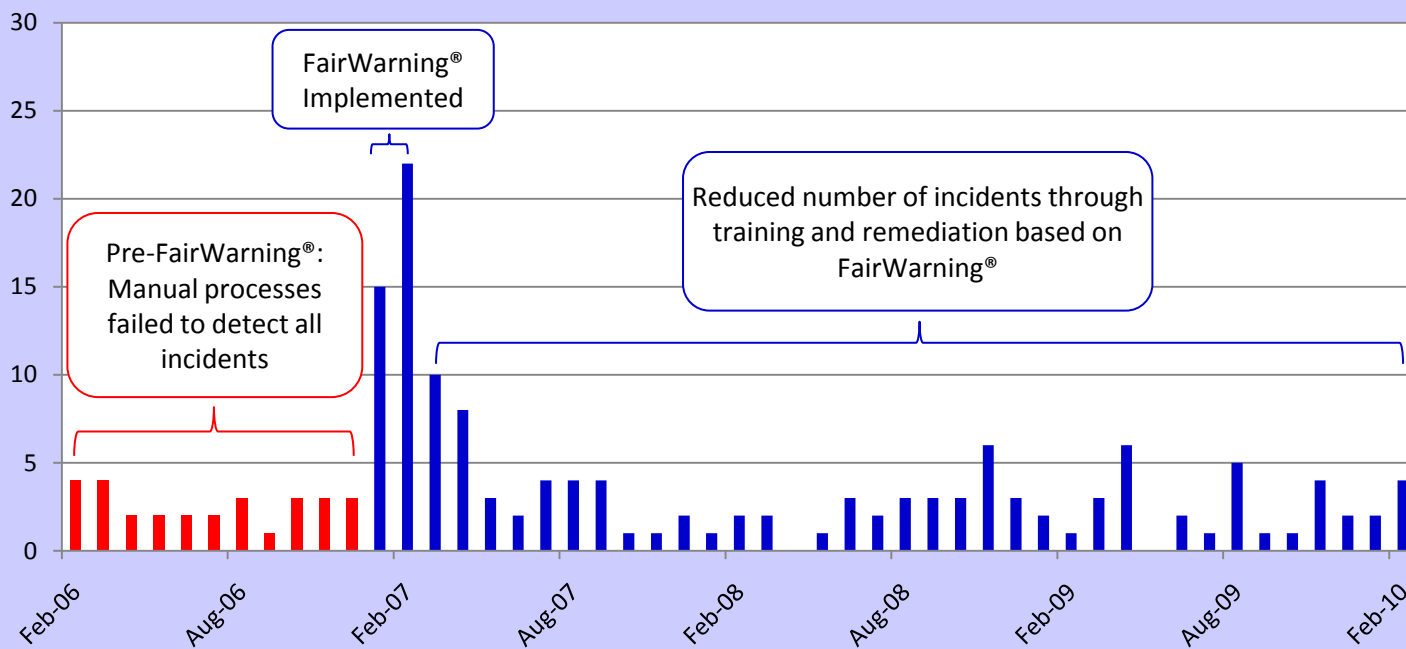


- Patient privacy breach detection, remediation, governance, ad-hoc reporting, enterprise security
- Best practices for:
  - Breach detection, notification, disclosure
  - Remediation and work-flow
  - Privacy & security audits
  - UK Data Protection Act, UK Human Rights Acts, UK Freedom of Information Act, Caldicott Guardian
- Automates systematic audit log review of all applications as required by NHS IGT
- Alert on 100+ patient privacy scenarios with filtering  
Deters snooping, medical identity theft, identity theft
- 100+ EHRs and healthcare applications supported out-of-the-box
- Out-of-the-box, in-production, massive scale, patents pending

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



### Inappropriate EHR Access - Confirmed Incidents



## ROI - 10X reduction in privacy audit review time

Reviews reduced from 5 days / week to ½ day / week

Confirmed privacy incidents reduced 86%

Personnel re-focused on training, education, research

Personnel re-focused on upcoming security projects



# Recent United Kingdom healthcare privacy news



**BBC NEWS** | 11:00 AM GMT, Friday, 3 September 2010

## Who is looking at your medical records?

It's been 10 years since the NHS introduced the idea of people viewing their own medical records online. But how many people are actually doing so? And how many are looking at records that aren't theirs? The NHS is trying to find out.

From 100,000 people in 2000, the number of people who have viewed their records has risen to 1.5 million in 2009. But the NHS is still trying to work out how many people are looking at records that aren't theirs. It's a big job, because the NHS has to make sure that people can only see their own records. And it's also trying to make sure that people can't see records that they shouldn't be able to see.

The NHS is trying to find out how many people are looking at records that aren't theirs. It's a big job, because the NHS has to make sure that people can only see their own records. And it's also trying to make sure that people can't see records that they shouldn't be able to see.

**BBC NEWS** | 11:00 AM GMT, Friday, 3 September 2010

## NHS told to tighten up data security

The Information Commissioner has told the NHS to improve data security, after launching an inquiry into the loss of thousands of personal medical records.

The Information Commissioner has told the NHS to improve data security, after launching an inquiry into the loss of thousands of personal medical records. The NHS is being told to tighten up its data security measures to prevent such incidents from happening again.

The Information Commissioner has told the NHS to improve data security, after launching an inquiry into the loss of thousands of personal medical records. The NHS is being told to tighten up its data security measures to prevent such incidents from happening again.

**BBC NEWS** | 11:00 AM GMT, Friday, 3 September 2010

## 'Private and confidential'

Some 800,000 confidential journals have been stored in the NHS's medical records system. But how many people are actually looking at them? And how many are looking at records that aren't theirs? The NHS is trying to find out.

Some 800,000 confidential journals have been stored in the NHS's medical records system. But how many people are actually looking at them? And how many are looking at records that aren't theirs? The NHS is trying to find out.

Some 800,000 confidential journals have been stored in the NHS's medical records system. But how many people are actually looking at them? And how many are looking at records that aren't theirs? The NHS is trying to find out.

**BBC NEWS** | 11:00 AM GMT, Friday, 3 September 2010

## Thousands of patient details

Have been lost by the NHS in London following a series of data breaches, a report has revealed.

Thousands of patient details have been lost by the NHS in London following a series of data breaches, a report has revealed. The NHS is being told to improve its data security measures to prevent such incidents from happening again.

Thousands of patient details have been lost by the NHS in London following a series of data breaches, a report has revealed. The NHS is being told to improve its data security measures to prevent such incidents from happening again.

**eHealthInsider** | Primary Care | Europe | Jobs | Events

HOME | NEWS | DOCUMENT LIBRARY | FEATURES | OPINIONS & ANALYSIS | AWARDS | RESEARCH REPORTS | AWARDS | PODCASTS | VIDEO

## NHS has much to do on data security

16 June 2010

The NHS has much to do on data security and is still making "far too many" mistakes in securing patients' personal and sensitive information, says the Information Commissioner's Office.

The ICO says it remains highly concerned that data breaches involving people's personal information are continuing to occur in NHS organisations.

NHS Stoke on Trent and Basingstoke and North Hampshire NHS Foundation Trust are the latest NHS bodies that have been found to have breached the Data Protection Act.

NHS Stoke on Trent has been criticised for having potentially "destroyed or mislaid" about 2,000 paper physiotherapy records.

Basingstoke and North Hampshire NHS Foundation Trust, meanwhile, has been found to have emailed an Excel spreadsheet containing 617 patients' pathology results to a department with "no business need to have access to the excessive amount of clinical records."

The spreadsheet was not password protected and was sent via unsecured email.

The chief executives of both NHS organisations have signed formal undertakings outlining that they will process personal information in line with the DPA. The ICO says that a quarter of all data breaches reported to it are from the NHS.

Hick Gornil, head of enforcement at the ICO, said: "Everyone makes mistakes, but regrettably there are far too many within the NHS. Health bodies must implement the appropriate procedures when storing and transferring patients' sensitive personal information."

NHS Stoke on Trent will apply physical security measures in respect of paper medical records, particularly when they are in transit.

**ISOFT**

Next Generation LIMS

To find out more about ISOFT's solutions

Please click here

isofthealth.com

**system C**

Microsoft global partner of the year 2010 (Public sector, health)

Microsoft Learning deal

Orange brings Smartcontractors to UK

DfA says suspend access to GCs

King's makes progress on e-procurement

Pfizer to go in massive NHS reorganisation

Blood, medicines & assay tracking

# Example best practices privacy breach detection



## Regulatory Investigations and Auditing

- Individual patients
- Individual user
- GP / Physician
- Consultant / contractors
- Random patients
- Random users
- Others

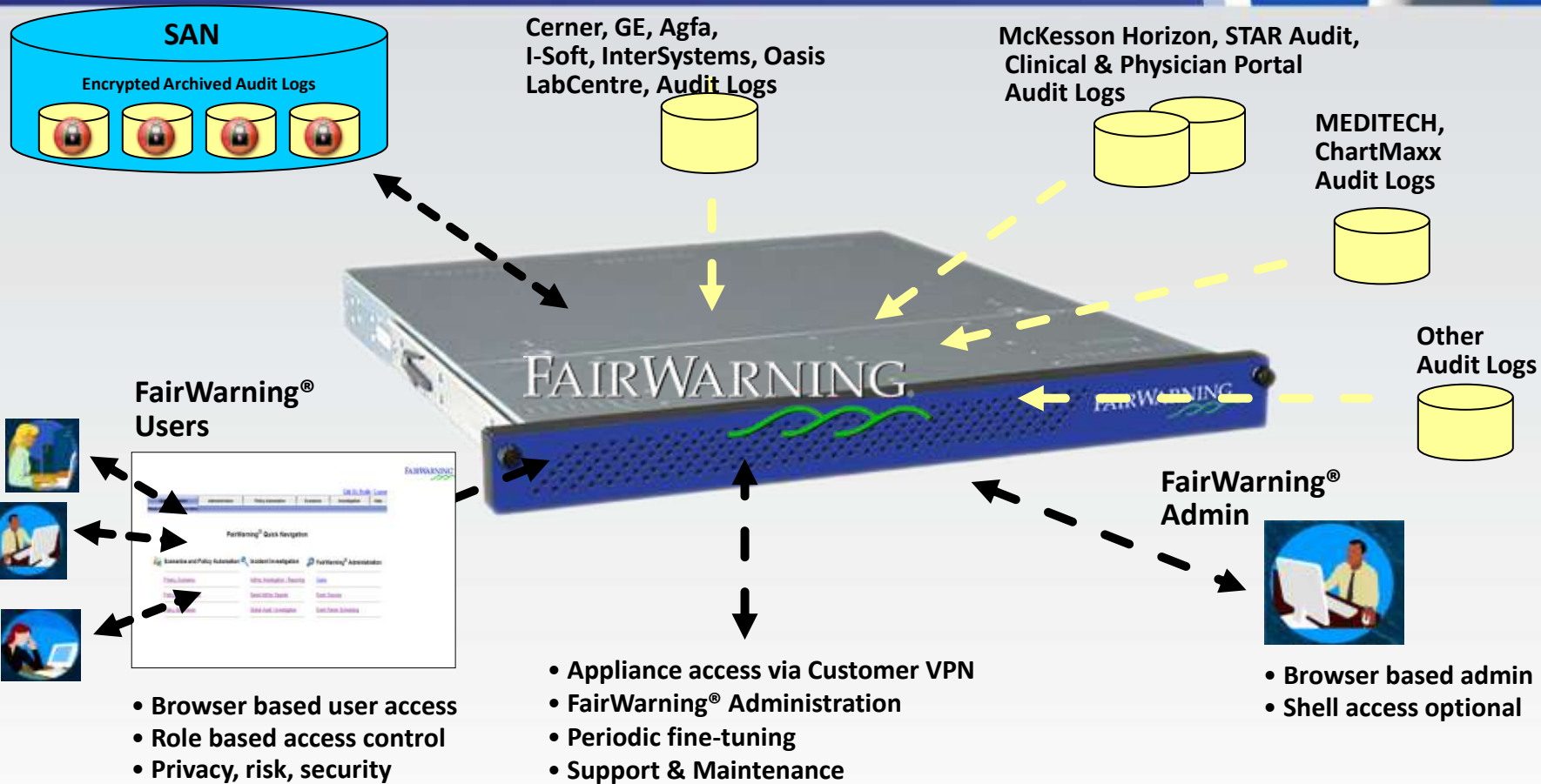
## Detecting “Snooping” Patterns

- VIP Scenarios: Prominent government officials, celebrities
- Family member snooping
- Employee as patient snooping
- Executive snooping
- Neighbor snooping
- Break-the-glass functions
- Self examination
- Others

## Other Snooping Patterns

- Sequential patient records
- Patient access thresholds
- Printed records thresholds
- Deceased patient records
- Discharged patient records
- Address changes
- Out-of-dept accounting, billing accesses
- Expired logins
- Simultaneous logins

# Example: System Architecture



# FAIRWARNING®

*Trust but verify®*



## NORTHGATE / NHS Lothian Case Study

# FairWarning® NHS Lothian



Sarah Emslie  
Client Director for Health

Mobile: +44 (0)7983 989514

Email: [sarah.emsle@northgate-is.com](mailto:sarah.emsle@northgate-is.com)

Web: [www.northgate-is.com/managedservices](http://www.northgate-is.com/managedservices)

 northgate  
MANAGED SERVICES

making IT work

© 2010 Northgate Managed Services Ltd

# NHS Lothian background

- NHS Lothian are the 2<sup>nd</sup> largest health board in Scotland and provide primary, community based and acute hospital services
- Lothian employ 28,000 staff which include 15,000 nurses and midwives and around 2700 medical staff
- Lothian have the 1<sup>st</sup> single “cradle to grave” Electronic Patient Record System incorporates A&E, Maternity, Outpatient services, Inpatient services, Radiology and Laboratory reports including Autopsy. This equates to approximately 850 000 patients and 1.3m records. The Lab system covers all of Lothian but with additional specialist services for the South East and central Scotland covering 1.5m patients.

# NHS Lothian systems

- There are 14,000 users of this electronic record, increasing to 18,000 over the next year
- NHS Lothian's Electronic Health Record systems have a comprehensive audit trail which produces large amounts of data. This data relies on a manual process of review which is extremely time consuming, costly and exposed to human error, thereby increasing the risk of government penalties, breach of patient trust and personal or organisational liability.
- Several high profile inappropriate incidences
- No ability to proactively monitor access

# FairWarning

- Northgate provided NHS Lothian with a Privacy Surveillance solution; the first health board in the UK to benefit from the solution.
- The FairWarning® surveillance software processes the massive amount of records from multiple healthcare applications by pulling audit files from each system identified by NHS Lothian to be monitored. These include the TRAK, SCI Store of digitised patient records, Emergency Care Summary, HR system and will shortly include a new clinical portal system

# Results

- Within the first hour of go-live NHS Lothian received their first set of users potentially breaching the access policy.
- Proactive monitoring enables NHS Lothian to review in advance anything likely to be deemed as a data protection breach and take steps to further prevent incidents occurring. It reduces privacy incident rates and enables a rapid and thorough response to patient privacy enquiries.

# Results

- The FairWarning® surveillance software processes the massive amount of records from multiple healthcare applications by pulling audit files from each system identified by NHS Lothian to be monitored. These include the TRAK, SCI Store of digitised patient records, Emergency Care Summary, HR system and will shortly include a new clinical portal system

# Results

- “The introduction of FairWarning as an addition to our existing capabilities has allowed us to significantly move ahead as we strive to ensure compliance with the DPA and provide assurance to our patients that their data is in safe hands.”

Martin Egan, Director of eHealth

- “The integration of FairWarning with the Emergency Care Summary (ECS) in Scotland will be a major step forward for boards in meeting the strict audit protocol requirements for ECS. FairWarning will make it significantly faster and easier for all accesses to be monitored and reported on and this will have significant benefits for ensuring the secure use of patient information in the NHS in Scotland.”

Jonathan Cameron, ECS Programme Manager, National Services Scotland

# FAIRWARNING®

*Trust but verify®*



FAIRWARNING®

PRODUCT DEMONSTRATION

# Privacy monitoring Resources



**Les Baker**  
Director of UK Sales

**Tel : 0800 047 0933**  
**Email: [Les@FairWarningAudit.com](mailto:Les@FairWarningAudit.com)**

- Customer case studies: [Patient.Privacy@FairWarningAudit.com](mailto:Patient.Privacy@FairWarningAudit.com)
- UK webinar on privacy monitoring: [Click here](#)
- Privacy monitoring white paper: [Click here](#)
- FairWarning® compatibility with SIEMs white paper: [Click here](#)
- Return on investment calculator: [Patient.Privacy@FairWarningAudit.com](mailto:Patient.Privacy@FairWarningAudit.com)
- Comparison & evaluation forms: [Patient.Privacy@FairWarningAudit.com](mailto:Patient.Privacy@FairWarningAudit.com)
- Planning & deployment guide: [Patient.Privacy@FairWarningAudit.com](mailto:Patient.Privacy@FairWarningAudit.com)