The Evolution of NHS Scotland into a World-Class Healthcare Provider

FairWarning® Executive Webinar Series
15 May 2013
Today’s Panel

Dr. Daniel Beaumont
Information Assurance Lead
Scottish Government (Health)
Daniel.Beaumont@scotland.gsi.gov.uk

Ian Merritt
Information Governance Lead
NHS Borders
Ian.Merritt@borders.scot.nhs.uk

Tim Dunn
Executive Vice President
FairWarning® Software Limited
Tim.Dunn@FairWarning.com
A New Era for Healthcare in the United Kingdom
Major Change in Healthcare Markets: In UK and Internationally

- The Patient has more power - where they go for treatment, who can see their records
- Commercial viability and competitive strength are a reality for federal run healthcare systems, as well as private sector markets
- Fraud is becoming a major global concern and healthcare is seen as an easy target
- Electronic (paperless?) records are critical to effective 21st century healthcare
- Regulation, audits and penalties are increasing at a UK, European and International level
What’s Next for the NHS?

• Is the NHS ready to become “best in class” globally for Health Service Delivery?

• How can the NHS offer patients an integrated National Service?

• What is the current state in NHS and what needs to happen next to meet the challenges and opportunities?

• What role will Information Governance play in the evolution of the NHS (and where should it sit in the priorities)?

• What impact will Caldicott 2 and the Francis Report have on Information Governance teams?
Using privacy breach detection tools as part of an Information Assurance Strategy:

Case study of NHS Scotland and FairWarning®

Dr. Daniel Beaumont
Information Assurance Lead, Scottish Government (Health)

Ian Merritt (Information Governance Lead, NHS Borders)
What is NHS Scotland?

- National Health Service (NHS) one of the most recognisable brands and UK citizens can avail of it wherever they are

- **BUT** health is a devolved area and there are now many differences in how health is funded and organised in the four parts of UK

- Overall policies on confidentiality are broadly the same, but there are differences in how England, Northern Ireland, Scotland and Wales approach improving standards in confidentiality

- NHS Scotland has 22 health boards (14 in territorial areas) 165,000 employees and 5 million+ patients in Scotland
NHS Scotland eHealth Strategy

1) To maximise efficient working practices, minimise wasteful variation, bring about measurable savings and ensure value for money

2) To support people to communicate with the NHS Scotland, manage their own health and wellbeing, and to become more active participants in the care and services they receive

3) To contribute to care integration and to support people with long term conditions

4) To enhance the availability of appropriate information for healthcare workers and the tools to use and communicate that information effectively to improve quality

5) To improve the safety of people taking medicines and their effective use

6) To provide clinical and other local managers across the health and social care spectrum with the timely management information they need to inform their decisions on service quality, performance and delivery
In order to explain why we invested in FairWarning® it is worth giving background on overall information assurance strategy:

- Trust is a massive building block in health care, and once lost, is difficult to recover.

- Without trust, there is less ability to do data sharing between organisations and more ambitious things in ehealth (“if you misuse my data in the hospital then why should I consent to online access etc.”)

- Do need to make clearer to patients that in modern healthcare there are a very large number of participants (medical and administrative) who have a legitimate need to access.
What is legitimate access?

- NHS Scotland policy on what constitutes legitimate access: one can see these a bit like ten spokes on a wheel....
So how much access is inappropriate?

- NHS has poor press regarding handling personal data
- Staff fully aware of Internet monitoring, but still perceive that other IT access is not checked
- Common view: “the system allows me to see the data; so surely I can therefore chose to access anything on it.”
- This can easily lead to complacency and despair: “culture is so bad; genie is out the bottle, nothing can be done to get people to respect confidentiality in the workplace....”
Ignoring...is accepting defeat

There are three reasons why we cannot simply park this issue:

1) Issue is just too important (Hippocratic Oath) and confidentiality and trust are key building blocks of health care

2) Examples in other sectors where there was similar problem and has been markedly improved (e.g. police national databases)

3) Vast majority of NHS staff are honest and trustworthy and it is they who want us to crack down on the minority who misuse data
What types of control would not work?

- Relying totally on guidance and training and no technology [this would be too complacent; given what we know about scale of problem]

- Other extreme, relying on technology with strict locked down role-based access approach [has been tried in England and elsewhere, and has been shown to be bureaucratic and almost unworkable]
‘Permission’ does not = technical permission

- Scottish strategy here takes view that a ‘permission’ (backed up the access wheel shown earlier) is not always the same as ‘technical permission’

- This is because the health care applications need that degree of flexibility (i.e. you change roles almost every hour, so should not need to keep ringing IT or your manager)

- But, with this flexibility – a trust based IT landscape – comes the higher risk of inappropriate access

- So, how do you reduce this risk while maintaining the benefits of wider access through tools like Single Sign On and Clinical Portals?
Part of the answer is more robust audit/reporting

But there are some barriers here:

1) Some of the oldest apps do not have useful audit trails

2) Majority of apps which do, have a super-abundance of data which is not easy to extract and interpret. Additionally, it is very time consuming finding information on specific individuals.

3) An audit trail does not of course give an ‘early warning’; it is something you tend to go to after the event.
What were we looking for in procurement?

- Get good reports, which are meaningful and could pre-empt misuse
- Easy to set up, ease of use, flexibility to tailor reports
- Will take minimal amount ISO’s time
- A tool which could, in conjunction with training, have best chance of changing behaviour for the better
FairWarning® chosen

- National license (so it can be used by all health boards)
- All territorial boards at different stages of implementation
- NHS produced implementation pack
Early decisions and actions...(1)

- How are you going to communicate with staff, HR, unions?
- Who is going to run the tool (IT security officer?)
- Which clinical apps are you going to link up to FairWarning®?
- Which of those apps acts as the identifier for staff?
- Which reports do you want (FairWarning® offers thousands of permutations such postcode employee/patient exact match)?
- How often to run reports (daily, weekly, monthly) to ensure data is not too voluminous to handle?
Early decisions and actions..(2)

- How are you going to filter for false positives?

- Are you going to send potential breach info direct to line managers, HR or somewhere else (if line managers how do you know who they are)?

- Have HR processes been adapted to cope with higher volumes of cases, to do triage?

- How are you going to do the quantitative analysis, and plot out graphs which show positive changes in behaviour?
Early lessons learned

- Perception that FairWarning® is more difficult to put and resource intensive than it really is (this has meant implementation has been put in a queue behind projects which have a more obvious front-line benefit such as SSO).

- HR concerns about opening lid on a “whole can of worms” and not being resourced to deal with it.

- Need to reassure people that after initial investment, potential breaches (and therefore work for all concerns) begin to diminish as word about FairWarning® gets around and letters are generated.

- Massive deterrent factor.
NHS Borders

- The Experiences of NHS Borders
- Lessons Learned
About NHS Borders

1 Ayrshire and Arran
2 **Borders**
3 Fife
4 Greater Glasgow and Clyde
5 Highland
6 Lanarkshire
7 Grampian
8 Orkney
9 Lothian
10 Tayside
11 Forth Valley
12 Western Isles
13 Dumfries and Galloway
14 Shetland
Implementation

Project Board
- Information Governance
- IT Resource
- Developers
- HR/Partnership
- Communications
- Clinical Representation
Method of use

- Scenarios
  - Surname
  - Address
  - Colleague

- False Positive Check

- Mail to Line Manager
  - Guidance developed
Process Flow

**FairWarning Incident Management Process**

1. **Clinical Systems**
   - FairWarning reports run daily
   - Reports Reviewed and Rationalised
   - Line managers and System Managers identified
   - Information Governance Team perform initial investigation
   - Recorded in Master Spreadsheet. Line manager advised
     - IG and System manager to provide logs from host system
     - Line manager to investigate further and respond to IG within 1 week
     - Incident confirmed
       - Yes: Master Spreadsheet updated
       - IG to advise HR. Senior management notified as necessary
       - Line manager records incident in DDB and consults with HR as appropriate
       - Standard HR processes and PIN Guidelines followed
       - HR to advise IG if "Action taken" or "No action necessary"
       - Periodic summary report prepared with statistical information
     - No: Master Spreadsheet updated
   - Yes: Potential Incident
     - No: Recorded as False positive
Findings

- Lots of False positives
  - Rural location
  - Local communities
  - Common surnames

- Some actual incidents
  - Self look-ups
  - Being helpful

- HR Involvement
Incidents trends

Incident Totals

Number of incidents

Week number

Investigated
Confirmed Incidents
Incident types

Incidents by type

Postcode  Self  Family Member  Co-Worker
Final thoughts...

- We agree with the ‘strap-line’ of the FairWarning® tool (which is to ‘Trust but Verify’), to have set of tools with maximum amount of flexibility/trust to help us with our strategic aims to provide better access to health-care data.

- But also to create an IT landscape where there is robust audit and a very powerful deterrent to any inappropriate access *(even when it is only technically possible to monitor a minority of applications)*.

- Choose carefully which FairWarning® reports are created as some have proven to be much more useful than others in health boards.

- Integrate into the normal working week of an information security professional.
Keep an eye on future potential of FairWarning®

- Often a privacy breach investigation leads to awareness of other things going on (e.g. workplace bullying, misuse of other IT tools, fraud, etc.)

- We still have a challenge in tying up evidence from different ‘workplace spheres’ (e.g. privacy breach data from FairWarning®, audit trails from IT apps not monitored by FairWarning®, internet and telephone usage data, CCTV, swipe card data, etc.)

- IT security officers, physical security officers, HR and Finance need to start working together much more closely

- Need to think how we get an early warning of behaviour that leads to financial crime, collusion with those seeking to carry out identity thefts, etc.
Dr. Daniel Beaumont  
Information Assurance Lead  
Scottish Government (Health)  
[Email Link to Daniel.Beaumont@scotland.gsi.gov.uk]

Ian Merritt  
Information Governance Lead  
NHS Borders  
[Email Link to Ian.Merritt@borders.scot.nhs.uk]

Tim Dunn  
Executive Vice President  
FairWarning® Software Limited  
[Email Link to Tim.Dunn@FairWarning.com]