



FOR IMMEDIATE RELEASE

Nationwide Survey Reveals Demand by Patients for Medical Record Privacy Guarantees Against Security Breaches

Report details that patients postpone seeking treatment out of confidentiality concerns

London, UK – 13th October 2011 – FairWarning Inc – the inventor and world’s leading supplier of cross-platform healthcare privacy auditing solutions for electronic health records (EHRs) - today released the findings of a major survey which reveals overwhelming demand for patients’ medical records to be guaranteed against data theft and snooping. The independent poll of 1,001 respondents showed that patients believe that hospital chief executives and top managers should be held accountable for healthcare privacy protections and breaches.

The survey also revealed that confidentiality concerns could have a direct impact on people’s health. Nearly four in 10 said they have, or would, put off seeking treatment, and well over half, have or would withhold information from clinicians, if a hospital had a poor reputation for security. Many respondents stated that they would travel substantial distances (37% would go 30 miles or more) to avoid being treated at a hospital they did not trust, in order to keep sensitive information confidential.

Kurt Long, founder and CEO of FairWarning[®], said: “Modern patient care is very much information-based. Any obstacle to the free flow of information between care providers and patients, such as those caused by privacy concerns, can prevent patients from receiving the best possible care. Patients across the UK have enormous faith in the NHS, but this survey reveals that more needs to be done for medical information to be shared and exchanged securely, and so to ensure the best patient outcomes.”

The survey showed that patients are worried that sensitive medical and personal information could be stolen and used by criminals for theft or fraud, or disclosed to employers or family – with serious consequences for their careers or relationships.

Most of those taking part in the poll had high demands of what the NHS should deliver in terms of confidentiality, wanting effective monitoring and firm enforcement of regulations. They also revealed that leaks and theft of personal data could do huge damage to the reputation of the health service. A large majority wanted access to their records to be strictly controlled and want to see strong deterrents to prevent further breaches.

The main findings of the survey included that:

- **87.1%** agree that chief executives and senior management should be sacked or fined if they were aware of risks but failed to act and there is a serious breach. Only **1.3%** disagree.
- **73.3%** felt that better enforcement of rules and regulations would cut security breaches.
- **62.1%** approve of having national league tables to show the best and worst hospitals for data security – only 9.7% disapprove.
- **86.5%** think that a serious breach of personal data would do severe or considerable damage to a hospital’s reputation.

- **87.2%** strongly or somewhat agree that the NHS should monitor who looks at their files.

The survey reveals that confidentiality concerns have a direct impact on the outcomes of care, and that patients were concerned about how their records could be misused:

- Over **61%** were very or somewhat worried that their identity could be used to commit fraud or used by criminals to target them, their family or home.
- **53.6%** have, or would, withhold information about a sensitive personal medical matter from a healthcare provider with a poor record of protecting patient privacy.
- **38.3%** have, or would, put off seeking care for a sensitive medical condition due to privacy concerns.

A total of 41 UK respondents (over 4%) claimed their medical records had already been breached. Some had information used against them in legal actions, had their identities stolen and suffered financially. However, 75.5% of UK patients said they value electronic records as a way for clinicians to share information and keep it up-to-date.

Where FairWarning[®] has introduced privacy breach detection and auditing solutions to monitor electronic records systems, the levels of staff snooping into patient files with no professional reason to do so, has been reduced by an average of 97%.

For a full copy of the survey results and methodology, please visit <http://www.fairwarningaudit.com/documents/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf>.

Ends

Survey objectives

FairWarning[®] commissioned the nationwide survey to examine how privacy concerns impact patients' healthcare decisions and more specifically measure to what degree privacy considerations influence:

- From whom patients seek care.
- When patients receive care.
- Where patients seek care.
- What information patients disclose, thereby affecting the care they receive.
- To what degree healthcare executives should be held accountable for privacy protections and privacy breaches.

Further survey findings

Management issues

- **97.1%** believe NHS chief executives and top managers have a legal and ethical duty to protect their data.
- **90.5%** agree that where there are significant risks of privacy breaches the chief executive and top management should take appropriate action to minimise or eliminate them.
- **87.3%** say that personal data breaches would make them think a hospital was badly managed.
- **77%** believe that chief executives and top managers should do more to stop unauthorised accessing of medical records.
- **75.5%** value electronic records as a way for clinicians to share information and to keep information up to date.

How breaches harm the NHS

- **72.9%** said that serious or repeated privacy breaches would reduce their confidence in the quality of care provided by a hospital.
- **61.5%** stated that personal information breaches would make them want to seek treatment at another hospital. Of these people **37%** would travel 30 miles or more, including **12.4%** who would travel 50 miles or more.

Rules and regulations

- **73.3%** felt that better enforcement of rules and regulations would cut security breaches.
- **55.8%** feel that existing laws are not adequately enforced.
- **62.1%** approve of having national league tables to show the best and worst hospitals for data security – only 9.7% disapprove.

Reputation of the NHS

- **63.2%** believe the NHS is committed to protecting their personal data.
- **29.4%** do not believe their hospital/healthcare provider has proper privacy safeguards.

Tough consequences for patients who had experienced breaches

- Of the 41 patients (4.01%) who knew their records had been breached 4 said it was by a friend, 9 a family member, 6 a co-worker and 6 a healthcare worker unknown to them.
- Eight said they were the victims of identity theft, 2 had private information used against them in a law suit, and 6 became the subject of gossip.
- Three people reported serious financial consequences, 1 lost their job, 8 needed credit monitoring to protect against crime, 5 had incorrect medical information added to their files and 9 had to invest significant time and effort in putting the situation right.
- Some 28 were informed within 30 days of the breach, though 4 found out themselves.
- Healthcare providers' responses were viewed positively with 29 people saying they were satisfied or very satisfied.

Notes for editors

The survey was carried out by New London Consulting and took place in the nine day period from Thursday, August 25, 2011 to Friday, September 02, 2011 inclusive. Separate breakdowns of the results can be provided for England, Scotland and Wales. They are also available for London and the South East, the South West, the East of England, East and West Midlands, the North East, North West, Yorkshire and Humberside. The results from similar research carried out in the USA in July 2011 are also available.

About FairWarning, Inc.

FairWarning[®] is the world's leading supplier of cross-platform healthcare privacy auditing solutions for Electronic Health Records. FairWarning[®] proactively protects healthcare organizations from emerging legal and privacy threats which include medical identity theft, identity theft, and other forms of healthcare information crimes. FairWarning[®] is industry's leading best practice solution for automating privacy auditing. The company is located in St. Petersburg, FL, with offices in London, England and Paris, France. To learn more, visit <http://www.FairWarningAudit.com>

Media Contacts

Interviews with Kurt Long are available on request. A photo is available from

<http://www.fairwarningaudit.com/subpages/Management.asp>.

Please contact: Susan Venables, Highland Marketing on behalf of FairWarning

Tel: +44 (0) 1877 339922 / Mobile: +44 (0) 7971 166936 email: susanv@highland-marketing.com