



FOR IMMEDIATE RELEASE

Aintree University Hospital NHS Foundation Trust Selects FairWarning[®] Solution to Bolster Patient Privacy

*Trust's increasing reliance on electronic health records provides catalyst for deployment of
privacy monitoring solution*

LONDON, UK – 16 July 2012 – One of the most proactive NHS trusts in England in terms of its innovative use of information technology, has selected [FairWarning[®]](#) Privacy Breach Detection solution to counter the growing threat of serious data breaches and the improper accessing of electronic health records (EHRs).

[Aintree University Hospital Foundation Trust](#), which is recognised as having developed one of the most advanced IT architectures in the NHS – with around 90% of its health records being electronic – plans to deploy the FairWarning[®] solution across all of its clinical systems.

The move reflects the NHS's increasing reliance on EHRs to improve patient care, but acknowledges the need for trusts to monitor and protect patient privacy in order to capitalise on the opportunity. Ward Priestman, Director of Informatics and Senior Information Risk Officer at Aintree University Hospital, noted that the evolution of electronic healthcare had made implementing a privacy monitoring solution essential.

"There is a sea-change in the depth of data that is now being recorded electronically," he said. "Previously, most confidential information was on paper, locked in secure storage and well managed. But now that we're starting to record an increasing amount of clinical and confidential data on electronic systems, the thinking has got to mature. Solutions such as FairWarning[®] are going to be imperative."

Aintree was one of the first NHS Trusts to implement an electronic patient record (EPR) and has since gone on to develop an impressive informatics infrastructure. "Health records at the Trust are almost entirely electronic – we have engineered over 90% of the paper out of the organisation," said Priestman. "But with electronic systems it is much easier to access patient records *en masse*. We took the view that we needed to be more proactive in identifying breaches and have chosen to implement the FairWarning[®] system to enable us to monitor access efficiently and effectively."

The number of security breaches involving patient data has doubled in the UK in the past four years, with studies suggesting that the greatest threat to patient privacy comes from NHS staff abusing their legitimate access rights to electronic records. Countering the problem has historically been challenging. "Previously, the only way to address this was either through random audits or in response to a complaint. This was reactive, time-consuming and incredibly difficult to do," said Priestman.

"We needed a proactive, automated system that could tell us when people had been inappropriately accessing records. With FairWarning[®], staff will be aware that they are being monitored and, as such, inappropriate access should drop. It's a virtuous circle. Once a few breaches have been identified, people will recognise that the system is policing itself and the likelihood of individuals transgressing will reduce. They know they will be found out."

"Trusts need to do all that they can to maintain the confidentiality, integrity and availability of their systems to ensure that data is processed in a secure manner," said Neil Morgan, Information Security Manager at [Aintree University Hospital](#). "Audit capability has long been an issue with NHS systems. In order to protect

our data, we first need to understand how it is being used. What are the risks, what are the exploit vectors? Without a privacy detection solution, it's almost impossible to identify this. Now that we are implementing FairWarning[®], we will be able to monitor, identify and respond to what is going on. This is hugely advantageous.

“FairWarning[®] proactively identifies when a breach occurs. This will undoubtedly have the longer-term effect of reducing the number of breaches. It also fits into the ongoing development of our security architecture. FairWarning[®] enables us to move forward quite considerably. The greatest advantage of FairWarning[®] is that it can feed into more than one system, meaning we can integrate all of our clinical systems into this, and have one centralised system that can provide a high level of assurance to the Trust.”

Aintree plans to implement [FairWarning[®]](#) across its EPR, electronic document management system, digital radiology system, electronic prescribing system and its clinical portal.

The ability to demonstrate compliance is likely to become critical for trusts as they seek to establish strong public reputations in an NHS where patient choice and competition for services is increasing. Privacy monitoring solutions can help provide vital assurances that patient data is safe.

“It is good governance to take this approach – and more trusts should be doing it,” said Priestman. “Deploying FairWarning[®] is about further enhancing our local reputation and making sure that nobody loses confidence in our ability to manage secure data – whether they are business partners, commissioners, clinicians or patients. Ultimately, if patients and clinicians think that a system is insecure, they are not going to input sensitive data into it. And without that, electronic healthcare just won't work.

“There is no doubt that much more information will be made electronic over the next few years. The population is now much more demanding in terms of access to information, and the way technology has evolved means that is only going to increase. The whole of the NHS will have an electronic patient record within the next five years. This is exactly why trusts need to be on top of the privacy agenda.”

Les Baker, Country Manager of [FairWarning[®] UK](#), said, “As the health service continues to explore the undoubted opportunities of electronic healthcare, it is our hope that more NHS organisations follow the lead of proactive trusts such as Aintree University Hospital in recognising that sustainable data protection is the bedrock of success. Automated record monitoring and privacy breach detection solutions are readily available to the NHS – and they will be a key component in the successful delivery of the ambitious, but vitally important, NHS Information Strategy.”

ENDS

About Aintree University Hospital NHS Foundation Trust

Aintree University Hospital NHS Foundation Trust was established on 1 August 2006 as a public benefit corporation authorised under the National Health Service Act 2006. It is a large, complex organisation providing acute healthcare to a population of 330,000 in North Merseyside and surrounding areas. The immediate catchment covers some 33 square miles which is largely urban with significant areas of commerce including docklands. The Trust provides acute hospital services to the residents of South Sefton, North Liverpool and Kirkby.

It is also a teaching hospital for the University of Liverpool and a tertiary centre providing specialist services to a much wider population of around 1.5 million in Merseyside, Cheshire, South Lancashire and North Wales. The population served by Aintree includes some of the most socially deprived communities in the country, with high levels of illness creating a high demand for hospital-based care. For more information about Aintree University Hospital Trust, please visit <http://www.aintreehospitals.nhs.uk/>.

Information Governance Toolkit

Regulation relating to information security is largely dictated by the Data Protection Act (DPA), which underpins the guidance outlined in the Information Governance Toolkit. In recent months, the NHS has

come under greater scrutiny from the Information Commissioner's Office (ICO), which issued its first fine to an NHS Trust for a DPA breach at the end of April 2012.

About FairWarning, Inc.

FairWarning[®] is the inventor and world's leading supplier of cross-platform healthcare privacy auditing solutions for Electronic Health Records. FairWarning[®] proactively protects healthcare organisations 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 Clearwater, FL, USA with offices in London, England and Paris, France. To learn more, please visit <http://www.FairWarning.com> or call 0800 047 0933 or US +1 727 576 6700.

Media Contacts

Interviews with Les Baker are available on request.

Myriam McLoughlin

Tel: +44 (0) 1877 339922

Mob: +44 (0) 7940 549163

Email: myriamm@highland-marketing.com

Susan Venables

Tel: +44 (0) 1877 339922

Mob: +44 (0) 7971 166936

Email: susanv@highland-marketing.com