



**FOR IMMEDIATE RELEASE**

**CONTACT:**  
**FairWarning, Inc.**  
Sadie Peterson  
727 576 6700 x119  
[Sadie@FairWarningAudit.com](mailto:Sadie@FairWarningAudit.com)

**FairWarning® Releases Second Guide in Patient Privacy Framework:  
Patient Privacy in Enterprise Security Data Definition Guide for Wide-Scale  
Patient Privacy Auditing**

*The second guide outlines the integration of Privacy Breach Detection with Enterprise Security tools to offer Information Security officers complete visibility into potential privacy breaches*

**ST. PETERSBURG, FL – August 4, 2010** – FairWarning, Inc., a leading global supplier of cross-platform healthcare privacy auditing solutions for Electronic Health Records (EHRs), today announced the availability of the Patient Privacy in Enterprise Security Data Definition Guide. This is the second guide in the FairWarning® Patient Privacy Framework set of independent data definition guides for patient privacy breach detection and prevention in healthcare.

Healthcare organizations are using FairWarning® privacy breach detection solutions to monitor and audit potential privacy breaches within EHRs. The Patient Privacy in Enterprise Security Data Definition Guide details the cooperative correlation possible between privacy breach detection and Enterprise Security technologies, such as Security Information Event Management (SIEM) and Data Leakage Protection (DLP). This allows Information Security personnel to have complete visibility and correlation of suspicious application-level activity with other infrastructure activity, providing a comprehensive end-to-end forensic analysis of an incident.

“The FairWarning® Patient Privacy Framework will enable the uninterrupted promotion and adoption of EHRs by providing a practical working framework for enabling patient privacy on a wider scale,” said Kurt Long, CEO of FairWarning®. “This guide details the data necessary to perform advanced analytics and end-to-end traceability of access to electronic health records.”

FairWarning customers are reporting a dramatic reduction in the number of incidents occurring in their organizations, as a result of privacy auditing. The correlation possible between privacy breach detection and Enterprise Security tools further supports the protection of patient privacy.

“Southwest Washington Medical Center has seamlessly interfaced FairWarning® alerts into our ArcSight SIEM, allowing us to correlate breach threats across our service platform, networks and compliance program. You don’t know what you don’t know, until you have full-spectrum awareness across your service delivery suite. FairWarning® fills in the clinical application detail that is missing,” says Christopher Paidhrin, Security Compliance Officer at Southwest Washington Medical Center.

To request a copy of either the first or second guide in the FairWarning® Patient Privacy Framework, please email [Guide@FairWarningAudit.com](mailto:Guide@FairWarningAudit.com).

###

### **About the FairWarning® Patient Privacy Framework**

The FairWarning® Patient Privacy Framework is a series of three (3) practical documents intended to enable wide-scale patient privacy auditing, breach detection, remediation and breach prevention:

- 1. Patient Privacy Data Definition Guide** provides details on the data requirements and definitions necessary to conduct minimum and advanced levels of patient privacy auditing.
- 2. Patient Privacy in Enterprise Security Data Definition Guide** details the integration between privacy auditing and enterprise information security systems.
- 3. Putting the Patient Privacy Framework into Practice** details the best practices for privacy breach detection, remediation, training, and breach prevention. Available August 2010.

### **About FairWarning, Inc.**

FairWarning® is a global leader in appliance-based software solutions which monitor and protect patient privacy in electronic health records enabling healthcare providers and health information exchanges to confidentially connect physicians, clinics, patients and affiliates. FairWarning®'s turn-key privacy auditing solutions are compatible with healthcare applications from every major vendor including Allscripts, Cerner, Epic, GE, McKesson, MEDITECH, Siemens, and many others. Customers consider FairWarning® privacy auditing solutions essential for compliance with healthcare privacy regulations such as ARRA HITECH privacy and meaningful use criteria, HIPAA, EU Data Protection, UK Freedom of Information Act, California SB 541 and AB 211, and Canadian provincial healthcare privacy law. For more information on FairWarning® visit [www.FairWarningAudit.com](http://www.FairWarningAudit.com), email [Solutions@FairWarningAudit.com](mailto:Solutions@FairWarningAudit.com) or call 727 576 6700.