

FairWarning Foils EMR Privacy Breaches

Data definition guides help hospitals and healthcare offices detect, notify, and prevent privacy violations in electronic medical records.

By Nicole Lewis, [InformationWeek](#)

May 7, 2010

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=224701076>

FairWarning has developed data definition guides that the company says will help detect and prevent breaches of patient information in healthcare settings, a growing concern as the adoption of electronic medical records accelerates.

The St. Petersburg, Fla. firm supplies cross-platform healthcare privacy auditing for EMRs, and said it has deployed privacy, auditing, and monitoring solutions in more than 300 hospitals and 1,200 clinics across the United States, Canada, and Europe.

The FairWarning Patient Privacy Framework is a series of three documents that help hospital CIOs, IT managers, and other employees implement wide-scale patient privacy auditing, breach detection, remediation, and breach prevention, the company said.

The first document, the Patient Privacy Data Definition Guide, provides details on the data requirements and definitions necessary to conduct minimum and advanced levels of patient privacy auditing.

The second, Patient Privacy in Enterprise Security Data Definition Guide, describes the integration between privacy auditing and enterprise information security systems.

The third, Putting the Patient Privacy Framework into Practice, specifies the best practices for privacy breach detection, remediation, training, and breach prevention.

According to Kurt Long, FairWarning's CEO, the Patient Privacy Framework addresses specific privacy breaches which are defined in the American Recovery and Reinvestment Act.

"The definition of breach at the federal level in the ARRA HITECH legislation occurred in February 2009, with a final rule effective in August 2009. As a result, many healthcare organizations are unprepared to protect patient privacy on a wide-scale basis," Long said. "All of the definitions and best practices are related to this brand new definition and associated regulations," Long added.

Long said the FairWarning Patient Privacy Framework can enable hospital staff to detect incidents of snooping into VIPs' medical records.

"For example, a local government official checks into the hospital. Employees of the hospital are curious and access his records. Data definitions and best practices within the FairWarning Patient Privacy Framework would allow the hospital to receive an alert that these records may have been inappropriately accessed," Long said.

Another example Long cites is the vigilance that needs to be deployed when a hospital employee becomes a patient.

"Her co-workers are concerned about her status and access her records. Data definitions and best practices within the FairWarning Patient Privacy Framework would allow the hospital to receive an alert that these records may have been inappropriately accessed," Long said.

The FairWarning Patient Privacy Framework was developed in conjunction with the company's customers, which include Weill Cornell Medical College, the University of Pittsburgh Medical Center, and the University of California San Diego Medical Center. The company also has partnerships with security technology vendors such as Symantec, ArcSight, and NitroSecurity.