



May 4, 2010

## Firm Issues Breach Detection Lessons

FairWarning Inc., a vendor of privacy breach detection software for health care organizations, has released the first of three best-practice guidance documents based on its implementation experience with more than 300 hospitals and 1,200 clinics.

The documents reflect lessons that the vendor and its customers have learned as they sought the best ways of using data the software can collect, says Kurt Long, CEO at the St. Petersburg, Fla.-based company. The material is appropriate for provider organizations, software vendors, systems integrators and others who act as covered entities or business associates handling protected health information.

FairWarning's software automates privacy auditing and monitoring activities. The applications, for instance, can identify an individual accessing hundreds of records and printing them, or moving them to a flash drive. Audit logs collect and track such data as date, time, user, patient, function performed, campus location, bed, floor number, and where the function was performed. Security officers, for instance, can see that a nurse was accessing records when off shift or on a floor the nurse usually does not work on. Other collected data, such as gender, next of kin and address, enable the identification of patterns that could indicate an individual is searching records of neighbors or family members.

The industry has had best information security practices for many years, Long acknowledges. "But some of this is pretty new," he adds. "A privacy breach was only federally defined in February 2009 in the HITECH Act. So this is uncharted terrain for many vendors."

The three guides are free, but there certainly is a marketing angle to the offer, Long notes. By getting vendors and their customers on the same page, "we feel it sets the groundwork for us to sell more of our software."

The first guidance document, available now, is the "Patient Privacy Data Definition Guide," which details data requirements and definitions necessary to conduct minimum and advanced levels of privacy auditing. A second data definition guide for enterprisewide security is expected in June. The third guide being released in July, "Putting the Patient Privacy Framework into Practice," essentially is a training manual that is much more prescriptive than the first two guides.

More information is available at <http://www.fairwarningaudit.com>.

-Joseph Goedert