

HIPAA audits drive business for privacy software firm

By John Moore

Jul 23, 2008

FairWarning, a supplier of health care privacy auditing systems based in St. Petersburg, Fla., reported revenues for the first six months of 2008 more than doubled over the same period last year.

Company executives believe the increase has been due to a rise in electronic identify theft and snooping, as well as the announcement that the Department of Health and Human Services would start to audit hospital compliance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA),

In January, HHS's Centers for Medicare and Medicaid Services disclosed plans to audit 10 to 20 hospitals.

FairWarning, which was started in 2005, markets to hospitals, health systems and major physician offices. Kurt Long, the company's chief executive officer, said the company has also started working with regional health information organizations (RHIOs). FairWarning's involvement with RHIOs stems from the company's collaboration with such health care applications vendors as GE Healthcare.

"In general, what you've got is RHIOs starting to get their arms around auditing," Long explained, noting that until recently RHIOs were mainly focused on getting their baseline deployments up and running.

FairWarning recently added support for Audit Trail and Node Authentication (ATNA), a move the company said will assist RHIOs and health information exchanges in auditing computer-to-computer transactions.

ATNA is an integration profile from the Integrating the Healthcare Enterprise (IHE) organization. Long described ATNA as one mechanism through which the company "can provide a comprehensive picture of a patient, or of a user, in terms of audit."

Long said electronic health records vendors are architecting their products in the future around ATNA.

FairWarning's privacy audit solution, which runs on an appliance server, takes audit logs and auditable events from health care applications. The audit data is stored in a database, through which FairWarning looks for patterns that might indicate medical identity theft or a snooping scenario, Long said. The solution sends alerts to a dashboard, which allows a privacy officer to monitor threats.

About the Author

John Moore is a freelance writer based in Syracuse, N.Y.

