


Not your daddy's watercooler



**SHARK BAIT** BETA  
Cast your tech tidbits into the feeding frenzy

## COMPUTERWORLD Security

 Print Article  Close Window

### HIPAA audit at hospital riles health care IT

Industry on edge after feds examine data security procedures at Atlanta facility

Jaikumar Vijayan

**June 15, 2007 (Computerworld)** An audit of Atlanta's Piedmont Hospital that was initiated by the U.S. Department of Health and Human Services in March is raising concerns in the health care industry about the prospect of more enforcement actions related to the data security requirements of the federal HIPAA legislation.

The audit was the first of its kind since the Health Insurance Portability and Accountability Act's security rules went into effect in April 2005, joining data privacy mandates that were already in place. The security rules require organizations that handle electronic health data to implement measures for controlling access to confidential medical information and protecting it against compromise and misuse.

Neither Piedmont nor the HHS has confirmed that the audit was launched, and few details about it have been disclosed publicly. But an HHS document obtained by *Computerworld* shows that Piedmont officials were presented with a list of 42 items that the agency wanted information on.

Among them were the hospital's policies and procedures on 24 security-related issues, including physical and logical access to systems and data, Internet usage, violations of security rules by employees, and logging and recording of system activities. The document also requested items such as IT and data security organizational charts and lists of the hospital's systems, software and employees, including new hires and terminated workers.

The mere fact that an audit of HIPAA security compliance was conducted for the first time has many in the health care industry preparing for more enforcement actions, according to Barry Runyon, an analyst at *Gartner Inc.* "I don't think Piedmont was an anomaly," he said. "My sense is that there is going to be more feet on the street from HHS going on unannounced audits."

Randy Yates, director of security at Memorial Hermann Healthcare System in Houston, said the Piedmont audit contributed in a big way to the approval of a \$1.3 million budget item for data encryption during the health care provider's next fiscal year.

"Everybody is aware of the Piedmont audit notification," Yates said. He added that after hearing about it, "we did our own gap analysis and found out where we are at highest risk for noncompliance, and we have since taken steps to shore up [those areas]."

As part of its efforts to bolster security, Memorial Hermann is also rolling out access management tools developed by Courion Corp. in Framingham, Mass. Yates said the software is expected to help the health care system automate policies for controlling access to protected medical information by its 19,000 employees.

Also driving the increased focus on HIPAA compliance at Memorial Hermann is a directive issued last December by the federal Centers for Medicare & Medicaid Services (CMS), Yates said. The directive ordered entities that handle patient health information to implement stronger authentication mechanisms for controlling access to the data.

Yates expressed confidence about the measures taken by Memorial Hermann to comply with the HIPAA requirements. But he added that the lack of detailed public information about what the HHS was looking for at Piedmont "is a little bit disconcerting."

The fact that the audit appears to have been conducted by the Office of the Inspector General (OIG) at the HHS is puzzling, said Lisa Gallagher, director of privacy and security at the *Healthcare Information and Management Systems Society* in Chicago. She said most people in the health care industry had assumed that any security-related enforcement actions would be taken by the CMS, which administers the HIPAA security rules.

"Nobody really knows why the OIG did it or what's going to be their criteria for selecting the next one," Gallagher said. "There's a lot of buzz in the industry." In addition, she voiced concerns about the checklist approach that the OIG auditors seem to have taken with their request for information from Piedmont.

Officials at Piedmont didn't respond to a request for comment about the audit. An HHS spokesman said only that as a matter of general policy, the agency doesn't comment about ongoing audits.

Chris Apgar, president of Apgar & Associates LLC, a Portland, Ore.-based consulting firm, said he thinks the HHS decided to conduct the audit at least partly because it was getting political and media pressure to enforce the HIPAA rules. Apgar expects to see more audits going forward. But he said they're unlikely to occur very frequently, because the HHS simply doesn't have the required staffing



resources.

Despite the industry buzz cited by Gallagher, Apgar said he's skeptical that the audit at Piedmont will spur many health care organizations to step up their efforts to comply with the security mandates.

"Until at least several audits have been completed, and the industry sees action taken to enforce the HIPAA security rules, I think serious attention to compliance will not be a major focus," he said.

However, it isn't just enforcement by the HHS that health care providers and other organizations handling medical data need to be concerned about, said Peter MacKoul, president of HIPAA Solutions, a Sugar Land, Texas-based firm that offers tools and services to help companies comply with the law.

MacKoul said that increasingly, law enforcement authorities and courts are using and interpreting HIPAA in ways that could have broad implications for organizations handling health care data.

For instance, the North Carolina Court of Appeals last year overturned the decision of a trial court to dismiss a HIPAA-related complaint brought by an individual against a psychiatrist's office. The verdict basically allowed the plaintiff to use HIPAA as "a standard of care" to bring an individual action against an organization, MacKoul said.

In addition, he noted that HIPAA initially applied only to electronic medical records. But, MacKoul said, courts have extended the law to cover paper records as well -- a fact that some health care providers may not be aware of.