Health Information Compliance Alert

HEALTH INFORMATION NEWS: KATRINA EVACUEES' EMRs GO ONLINE

With more than 800,000 evacuees from the storm-ravaged Gulf Coast seeking treatment in designated shelters, the federal government launched electronic medical records to help providers better streamline patient care.

The records were compiled from various pharmacies and other providers and loaded into a centralized database available to all doctors practicing in the eight shelters set up to aid evacuees after the hurricane. Officials plan to add information from a variety of other health care organizations.

The system--which took about 10 days to organize--could save lives, said Dr. **David Brailer,** coordinator of health information technology for the Department of Health and Human Services, in a press release.

The Bottom Line: You can expect officials to debate whether to enhance the database after the residents are permanently resettled. That decision will play a key role in the industry's development of interoperable health care networks, experts say.

CMP Final Rule Now Expected In 2006

If you were surprised by the Department of Health & Human Services' decision to end the civil money penalty interim final rule, you won't be shocked to find they've pushed the expiration date back another six months.

HHS published its plan to move the interim final rule's expiration date from September 16, 2005 to March 16, 2006 in the Sept. 14 Federal Register. The change is geared to avoid any disruption in ongoing enforcement action while HHS develops a more comprehensive enforcement rule.

The Bottom Line: You can't ignore your privacy and security rule obligations, but a final enforcement rule allowing CMS to impose CMPs is not yet a reality.

Lock Up Your PHI-Laden Media

You cannot leave your workstations or other electronic media vulnerable to data theft.

That's the message Palo Alto, CA-based Children's Health Council sent Sept. 20 after sensitive data--including the mental health information for more than 5,000 patients--was stolen, the San Jose Mercury News reports.

The information was stored on a computer and backup tape stolen from the non-profit medical group over the Labor Day weekend. None of the data has yet been used to steal patients' identities.

The Bottom Line: One stolen computer containing your patients' confidential information is all it takes to expose your organization to a security breach.