

Healthcare IT News

Healthcare IT News

Medical identity theft remains problematic

By [Jack Beaudoin, Editorial Director](#) | 09/19/07 |

SAN FRANCISCO – Physician practices and hospitals must not let their guard down when it comes to HIPAA, just because no civil actions have been filed under the law to date. And although the Office of Civil Rights has yet to levy a fine against HIPAA offenders, providers should not underestimate the cost of a security breach.

"Failure to protect patient data is very expensive," Chris Apgar reminded healthcare security experts at ITSecurity World in San Francisco this week. And, he added, it is probably more costly than taking the technical and procedural steps necessary to comply with the law.

Apgar is president of Apgar and Associates, which provides security consulting services to the healthcare and financial services industries across the U.S. He is a member of the Workgroup for Electronic Data Interchange Board of Directors.

"HIPAA is not a one-time event," Apgar said. Compliance should be "an ongoing activity that includes assessing risks," taking adequate precautions and providing patients with all the details about how their information is protected.

Apgar's talk at ITSecurity World was timely – a report released earlier this week from the eHealth Vulnerability Reporting Program found that electronic health records remain open to security breaches. The program spent 15 months investigating EHR use at more than 850 provider organizations and included penetration testing of seven ehealth systems.

EHR data could be a prime target for identity thieves, Apgar said. Potential damage includes credit theft, but also medical insurance coverage denial, discrimination, employment issues, and delivery of inappropriate healthcare.

Beyond the damage that such breaches can cause to patients, the failure to secure personal health data has expensive ramifications for providers.

For example, Apgar said, when Providence Health System lost 365,000 patient records on unencrypted back up tapes, it cost the provider \$3 million just to notify those affected. It was fined \$95,000 under the state's consumer protection laws, took a direct blow to its reputation, and now faces a class action lawsuit.

Apgar noted that while there are technological solutions that claim to harden records against vulnerabilities, it might be a mistake to focus too much on outside threats. "Eighty percent of all security breaches come from your people," he said. "It's not the hackers."

Rather than focus on the technology, Apgar offered up a list of policy recommendations that might reinforce – or require – more secure behavior among healthcare providers and prevent medical identity theft. These include:

- Forcing patient notification for all breaches that result in any inappropriate release of medical information;
- Create financial incentives to help smaller organizations protect data and notify patients of breaches, while stiffening penalties for providers who fail to do so;
- Enforce existing laws and conduct more compliance audits;
- Require vendors to prove appropriate privacy and security controls before they are eligible to participate in federal or state contracting;
- Create a nationwide body similar to existing credit bureaus to assist patients after a medical identity theft. Such an organization would help to correct medical records affected by a theft.