news
233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601

phone »(312) 233-1100
fax »(312) 233-1090
web »www.ahima.org

FOR IMMEDIATE RELEASE

For more information, please contact:
Bridget Stratton
Public Relations
312-233-1097
bridget.stratton@ahima.org

Combating Medical Identity Theft

Journal of AHIMA analyzes the 'privacy crime that can kill'

CHICAGO – April, 3 2014 – Medical identity theft – defined as the fraudulent use of an individual's identifying information in a healthcare setting – can corrupt records with erroneous information and compromise care through incorrect diagnosis and treatment. It also has the potential to inflict significant financial harm and complications on patients, providers and insurers.

The story, "Combating the Privacy Crime That Can Kill," in the April issue of the *Journal of AHIMA* examines medical identity theft and highlights best practices that health information management (HIM) professionals can implement to help stop medical identity theft before it harms patients.

These best practices are described in a new publication released by the California Attorney General's Privacy Enforcement and Protection Unit. To produce the guide, *Medical Identity Theft: Recommendations for the Age of Electronic Medical Records*, the Attorney General's Office consulted with numerous leaders in the field, including experts from AHIMA.

The *Journal* article cited the most recent study from the Ponemon Institute, which found that there were more than 1.8 million medical identity theft victims in 2013, a 21 percent year-over-year increase.

"This is another opportunity for HIM professionals to demonstrate leadership by proactively building awareness of medical identity theft threats and developing and implementing a defined identity theft response plan," said AHIMA CEO Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA. "HIM professionals can also provide consumer education on the importance of monitoring statements from the insurance company and healthcare providers for erroneous information."

The report listed five specific signs patients should monitor to recognize possible medical identity theft:

- Receipt of a privacy breach notice from a healthcare organization
- Unknown item in an Explanation of Benefits statement
- Notice of reaching a health insurance benefit limit that you believe is erroneous
- Call or letter from a debt collector about an unfamiliar medical bill
- Questions about your identity or health conditions during an intake at a doctor's office or hospital

The rise in electronic health records (EHRs) – highlighted in the March *Journal of AHIMA* – offers the potential to reduce the risk of medical identity threat.

"The move to electronic medical records provides an opportunity to address this serious quality-of-care issue," California Attorney General Kamala D. Harris said in the *Journal* article. "There are lessons to be learned from other industries that have experience in detecting and responding to fraud in electronic transactions."

The authors of the article -- Harry Rhodes, MBA, RHIA, CHPS, CDIP, CPHIMS, FAHIMA, director of HIM Practice Excellence at AHIMA, and Joanne McNabb, CIPP/US, CIPP/G, CIPP/IT, director of the privacy education and policy in Privacy Enforcement and Protection Unit in the California Department of Justice – noted that "tackling the privacy crime that can kill requires collaboration among all healthcare industry stakeholders. The issues posed by medical identity theft should be taken into consideration as standards are developed for the healthcare infrastructure of the 21st century."

Also in this issue

The April issue of the *Journal of AHIMA* also includes:

- A look at lessons learned from the first six months of Omnibus Privacy Rule implementation efforts. The story, "Top HITECH-HIPAA Compliance Obstacles Emerge," details where covered entities are in their compliance efforts as well as the Office for Civil Rights ability to enforce the rules.

- The practice brief, "Managing a Patient's Right to Request Restrictions of Disclosures to Health Plans," provides guidance to assist organizations in complying with the Omnibus Rule's new restriction requirements.

Read these articles and more in the April issue of the *Journal of AHIMA* or online at journal.ahima.org.

###

About AHIMA
The American Health Information Management Association (AHIMA) represents more than 71,000 educated health information management and health informatics professionals in the United States and around the world. AHIMA is committed to promoting and advocating for high quality research, best practices and effective standards in health information and to actively contributing to the development and advancement of health information professionals

worldwide. AHIMA's enduring goal is quality healthcare through quality information.
www.ahima.org