FOR IMMEDIATE RELEASE

Contact:	Emilie Moghadam Fleishman-Hillard 202.857.2212 emilie.moghadam@fleishman.com	Susan Moerschel Kroll Fraud Solutions 615.320.9800 ext. 964 smoerschel@kroll.com

GAPS IN HOSPITAL SECURITY POLICIES PUT PATIENT DATA AT RISK, ACCORDING TO NEW REPORT

A survey of U.S. healthcare organizations suggests that the industry's focus on medical privacy and HIPAA compliance limits other patient data security practices

NASHVILLE, TENN. – April 8, 2008 – The healthcare industry's focus on medical privacy and compliance has fostered a lack of awareness around the frequency, cause and seriousness of patient identity theft, according to the 2008 HIMSS Analytics Report: Security of Patient Data commissioned by Kroll Fraud Solutions, a leading provider of data protection and identity theft response services. The report reveals a significant blind spot that hinders hospital efforts to contain the problem and reduce risk.

"Healthcare facilities are complex environments where information is stored and shared in a number of ways that are critical to patient well-being," said Brian Lapidus, chief operating officer of Kroll Fraud Solutions. "Until healthcare organizations expand their data security measures to address the threat of data compromise as well as privacy and compliance, patients will continue to be at risk."

Key report findings include:

- Regulatory loopholes in data management standards_ allow data breaches to go unreported, preventing an accurate measurement of frequency.
  - **Only 56 percent of breached organizations surveyed notified the patients involved**.
  - On average, **respondents ranked their familiarity level with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at a 6.53** (on a scale of 1-7, with 7 being the highest) and nearly 75 percent claimed a familiarity level of 7.
  - The high level of HIPAA familiarity stems from the commencement of audits and the resulting penalties for non-compliant facilities. The issue: **HIPAA compliance is an insufficient proxy for risk mitigation.**
- Security policies place a greater emphasis on preventing violation of privacy than preventing fraud and malicious intent.
  - Of those respondents who experienced a fraud-related breach, **62 percent identified the type of the breach as unauthorized use of information**, while **32 percent cited wrongful access of paper records**.
  - Noticeably **absent were breaches attributed to malicious intent** (i.e., stolen laptops/computers, deliberate acts by unscrupulous employees, and cyber attacks through the Internet).
- Healthcare organizations lack appreciation for the costs of a breach.
  - **Only 18 percent of breached organizations surveyed believed there was a negative financial impact**, even though the average cost of a breach is estimated to be as high as $197 per compromised record and $6.3 million per incident._

"The number one priority of U.S. healthcare institutions is saving the lives of those in need and rightly so, I might add," said Lisa Gallagher, senior director of privacy and security for the Healthcare Information and Management Systems Society (HIMSS). "But patient safety extends beyond clinical care. This data tells us that organizations must also broaden their data security and risk management measures to address the threat of patient data breach."

Among the 13 percent of respondents who revealed that their facility had experienced a data breach:

- **48 percent indicated that "reprimanding the employee" is effective breach response**, while **11 percent offer "education" as a solution**.
- **35 percent said that they did not change the organization's security policy after the incident**.
- **Identity theft is three times as likely to happen at a larger facility** (more than 100 beds) **than a smaller facility** (under 100 beds).

The report also indicates that healthcare organizations are focusing their security programs on employee education with nearly all respondents reporting that their organizations educate employees about the importance of maintaining patient data security. Almost **50 percent cited reprimanding or terminating the employee as an element of their organizations' breach response plan** and **35 percent of breached organizations surveyed did not change their security policies after the incident**.

"There's a dangerous assumption in the healthcare industry that education leads to policy implementation and change," said Mr. Lapidus of Kroll. "Best practices in data security cannot be achieved by employee training alone. Organizations must make data security a part of their DNA, reflected in every aspect of business operations."

Survey Methodology: A total of 263 healthcare industry professionals participated in this research conducted in January 2008. They included IT professionals (50 percent), Health Information Management (HIM) managers (21 percent) and chief security officers (12 percent), among others working in the area of information management. Most respondents were small to mid-sized healthcare facilities.

For a copy of the 2008 HIMSS Analytics Report: Security of Patient Data and for more information on best practices in healthcare data security, please visit: www.krollfraudsolutions.com.

_ i.e., Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley Act of 2002 (SOX) and Payment Card Industry Data Security Standards (PCI)

_ Source: Ponemon Institute's 2007 Cost of a Data Breach Study

About Kroll

Kroll, the world's leading risk consulting company, provides a broad range of investigative, intelligence, financial, security and technology services to help clients reduce risks, solve problems and capitalize on opportunities. Kroll Inc. is a wholly-owned subsidiary of Marsh & McLennan Companies, Inc. (NYSE: MMC), the global professional services firm. Kroll began providing identity theft solutions in 1999 and created its Fraud Solutions practice in 2002 in response to increasing requests from clients for counsel and services associated with the loss of sensitive personal information, and related identity protection and restoration issues facing organizations and individuals.

Since then, Kroll's Fraud Solutions clients have included Fortune 500 companies, non-profit organizations, and government entities dealing with healthcare, financial services, insurance, consumer service, and any activity involving the collection and use of personal information. Kroll's Fraud Solutions team presently serves over 10,000 businesses and millions of individual consumers. For more information, visit: www.krollfraudsolutions.com.

About HIMSS Analytics

HIMSS Analytics supports improved decision-making for healthcare organizations, and healthcare IT companies and consulting firms by delivering high quality data and analytical expertise. The company collects and analyzes healthcare organization data relating to IT processes and environments, products, IS department composition and costs, IS department management metrics, healthcare delivery trends and purchasing related decisions.

HIMSS Analytics is a wholly-owned, not-for-profit subsidiary of the Healthcare Information and Management Systems Society (HIMSS).