idexperts®

Press Release

Top 11 Trends for 2012 in Healthcare Data, According to Industry Experts

A Look Ahead Points to Increased Risks; Regulatory Expectations; Reputational Fallout

PORTLAND, Ore. — January 5, 2012 — Hospitals and healthcare organizations will need more than a couple of aspirin to ready themselves for 2012. Industry experts representing healthcare law, privacy, security, regulatory and data breach were asked to forecast healthcare data trends for 2012. The overall forecast? Protecting patients' protected health information (PHI) should be viewed as a patient safety issue. If the right actions are not taken, experts predict healthcare data breach will reach epidemic proportions this year.

2011 was the year when most physicians had mobile devices; when healthcare became one of the most-breached industries; and the Department of Health and Human Services Office for Civil Rights (OCR) cracked the whip with investigations and multi-million-dollar fines for organizations that didn't meet their patient privacy obligations.

Top 2012 predictions in healthcare data:

1. **Healthcare organizations will not be immune to data breach risks caused by the spread of mobile devices in the workforce,** according to Dr. Larry Ponemon, chairman and founder, Ponemon Institute. In the recent benchmark study, 81 percent of healthcare providers say they use mobile devices to collect, store, and/or transmit some form of PHI. However 49 percent of those admit they are not taking steps to secure their mobile devices.

2. **Class-action litigation firestorms are imminent,** says Kirk Nahra, partner, Wiley Rein LLP. Class-action lawsuits will be on the rise in 2012, as patients are suing healthcare organizations for failing to protect their PHI. 2011 saw several class-action lawsuits for organizations, some of which involved business associates, due to breached patient data. Regardless of the outcomes, these lawsuits are a significant risk and tremendous expense for companies affected by them.

3. **Social media risks in healthcare will grow**, according to Chris Apgar, CEO and president, Apgar & Associates, LLC. As more physicians and healthcare organizations move to social media to communicate with patients and promote services, the misuse of social media will increase as will the risk of exposure of PHI. Often healthcare organizations do not develop a

social media use plan and employees represent a significant risk, potentially exposing PHI through their own personal social network pages. These risks can lead to patient vulnerabilities, data breaches, civil penalties, loss of business and more.

4. **Cloud computing is not a panacea; technology is outpacing security and creating unprecedented liability risks,** suggests James C. Pyles, principal, Powers Pyles Sutter & Verville PC. With fewer resources, cloud computing is an attractive option for healthcare providers, especially as Health Information Exchanges (HIE) increase. However, privacy and legal issues abound, such as compliance with HIPAA privacy and security regulations and allocation of liability when a privacy breach occurs. A covered entity will need to enter into a carefully written business associate agreement with a cloud computing vendor before disclosing protected health information and should ensure that it has adequate cybersecurity insurance to cover the direct and indirect costs of a breach.

5. **Growing reliance on business associates will create new risks**, believes Larry Walker, president of The Walker Company. Economic realities will force healthcare providers to continue to outsource many of their functions, such as billing, to third parties or business associates (BA). However, BAs are considered the "weak link in the chain," when it comes to data privacy and security. 69 percent of organizations that participated in the Ponemon study have little or no confidence in their business associates' ability to secure patient data. Third-party mistakes account for 46 percent of data breaches reported in the study.

6. **Organizations risk reputation fallout**, according to Rick Kam, president and co-founder of ID Experts and chair of the American National Standard Institute's (ANSI) "PHI Project," a project to research the financial impact of a healthcare data breach. Identity theft and medical identity theft resulting from data breach exposure are causing patients financial and emotional harm, often resulting in patients seeking out different medical providers. According to the Ponemon study, the average lifetime value of one patient is more than $113,000.

7. **Mobile will explode in healthcare,** believes Christina Thielst, health administration consultant and blogger**.** The use of tablets, smartphones and tablet applications in healthcare is growing exponentially. Nearly one-third of healthcare providers use mobile devices to access Electronic Medical Records or Electronic Health Records (EMR/EHR) systems, according to a CompTIA study. Providers will need to balance usability, preferences, security and budgetary concerns, as well as adopt written terms of use with employees and contractors using personal devices at work.

8. **Increased emphasis on willful neglect leads to increased enforcement of HIPAA,** according to Adam Greene, partner, Davis, Wright, Tremaine LLP. The focus over the next year will be on the 150 HITECH Act audits and publication of the final rules implementing modifications to the HIPAA regulations. But the biggest changes may be at the OCR investigative level. Expect OCR to more aggressively pursue enforcement against noncompliance due to "willful neglect" starting in 2012, resulting in a sharp uptake in financial settlements and fines in the coming years. 2012 will be the year that OCR expects everyone's training wheels to have come off their privacy and security programs.

9. **Privacy and security training will be an annual requirement**, says Peter Cizik, co-founder and CEO, BridgeFront. Healthcare organizations have gotten better at putting procedures in

place, but staff are still not following them. Because the majority of breaches are caused by human error, not technology failures, targeted training and awareness programs are one of the most effective ways to prevent data breaches.

10. **Rise in fraudsters will increase fraud risk education**, according to Jonnie Massey, supervisor, Special Investigations Unit, Oregon Dental Service (ODS) Companies. Pressure, opportunity and rationalization: these three dangerous elements of the triangle can lead to committing a healthcare-related crime. During hard economic times, there are more fraudsters and more opportunities for them to gain or keep a healthcare benefit they are not entitled to. Educating those at risk for fraud and communicating consequences may deter someone from stepping over the line or help those at risk to prevent them from being a victim of healthcare fraud.

11. **Healthcare organizations will turn to cyber liability insurance**, according to Christine Marciano, president, Cyber Data Risk Managers LLC. As healthcare organizations continue to implement their EHR systems, they will consider options to protect themselves and their patients. When a healthcare organization or other HIPAA covered entity suffers a data breach the cost can be damaging not only to an entity's bottom line, but also to the reputation of its brand. With the increased vulnerabilities and as part of a data breach response plan, healthcare organizations will increasingly turn to a cyber security/data breach insurance policy.

These top forecasts support the *2011 Benchmark Study on Patient Privacy and Data Security*, by Ponemon Institute, that found the frequency of data breaches in healthcare organizations surveyed increased by 32 percent, costing the U.S. healthcare industry an average of $6.5 billion. For a free copy of the report, visit http://www2.idexpertscorp.com/ponemon-study-2011/

# # #

Media Contact:
Kelly Stremel
MacKenzie Marketing Group
503-225-0725
kellys@mackenzie-marketing.com