**Lessons Learned from 2011 Data Security Enforcement Activity**

***By Leslie Bender, IFCCE, CIPP, CCCO***
***General Counsel/CPO***
***The ROI Companies***
***www.theROI.com***

On February 22, 2011, the U.S. Department of Health and Human Services (HHS) issued its first civil monetary penalties under the Health Insurance Portability and Accountability Act of 1996 (and related regulations, collectively "HIPAA") against CIGNET in the amount of $4.3 million. The underlying HIPAA problems: CIGNET failed to respond to 41 members' requests for copies of their health information and failed to cooperate with HHS in its investigation, including a failure to respond to the members' HIPAA-guaranteed rights to obtain copies of their health information. Two days later Massachusetts General Hospital settled a pending HIPAA enforcement investigation by voluntarily paying $1 million and entering into a Corrective Action Plan to shore up its compliance efforts. In the Mass General situation the underlying HIPAA problem: an employee commuting left patient scheduling and billing records on 192 patients on a subway train, which records were never recovered. Two weeks later HHS unfolded a well developed plan to begin educating State Attorneys General on HIPAA to position the Attorneys General to flex the enforcement muscles they gained under the HITECH Act amendments to HIPAA at the state level. Although to date only Connecticut's Attorney General has brought a HIPAA enforcement action, with HHS' encouragement and educational workshops, all the Attorneys General will be prepared to enforce medical privacy using HIPAA's significant civil monetary fines. Earlier this month HHS announced a third "settlement" for $865,500 with University of California at Los Angeles Health System in response to complaints filed by two celebrities alleging UCLA HS employees were allowed to snoop into the celebrities' protected health information despite having no business reason to do so due to UCLAHS's weaknesses in its HIPAA compliancy.

These actions and HHS's April roll out of in-servicing of the Attorneys General signals an end to the "enforcer with a heart" era that has prevailed since enforcement under HIPAA began back in April, 2003. Congress and the media have consistently been critical of HHS and the Office for Civil Rights in particular for their weak approach to making the standards and specifications under HIPAA's Privacy, Security and Transactions and Code Sets Rules a reality.

When you consider the underlying facts in the three recently publicized enforcement actions, most businesses that deal in confidential consumer financial and health information would be hard-pressed not to experience concern over incurring formidable fines and penalties from a regulator in a situation in which a consumer's request for information is inadvertently overlooked or a situation in which a well-intentioned employee takes work home and misplaces a file or record. These are essentially human errors that despite the best of intentions can occur.

Meanwhile, literally tens of thousands of websites encourage internet surfers to share or "disclose" information, blow the whistle on suspected bad actors – sometimes with offers of cash rewards -- and social networking sites, blogs, the proliferation of phones containing still and video cameras create an environment in which some of your organization's most precious and proprietary secrets and confidential information can find its way into the public domain in milliseconds.

Recognizing that it is impossible to conduct a healthcare related business without sensitive consumer information and without proprietary tactics and strategies, what can and should you think about doing to minimize the risk that what you wish to retain in confidence stays that way? To follow are five practical suggestions:

**1.Take the Laws and Regulations, Including Privacy and Data Security Laws Seriously**. While it will never be possible to eliminate all risks of improper disclosure of that information you do not want disclosed, it is critical for you to be familiar with what you are expected to do under state and federal laws and to use the standards and specifications in those laws as the foundation and structure of your compliance efforts. It is not necessary for your workforce to be able to recite the specific laws

and regulations, but it is necessary for them to have a working knowledge, practically related to their jobs and positions of these laws.

**2.Believe that One Employee's Poor Judgment or Error can Expose you to Significant Risk**. Nobody from the top executive to the part time summer hourly employee is immune from exposing your organization to significant risk if that person fails to recognize his/her individual responsibility for preventing or reporting a privacy or security incident. When you design compliance or training programs, assure everybody is included.

**3.Never Underestimate the Value of Training and Documentation**. Numerous studies document the value of training. Not only is it documented that employees working in companies that invest in appropriate training tend to stay in those companies and remain productive in those companies longer than employees in companies that do not, but companies that invest in meaningful training experience considerably lower costs in fines and penalties, distraction from core competencies to react to problems and waste less time on re-work – not to mention experience lower customer churn. According to a recent IBM analysis, the three categories where training can provide a measurable return on investment are revenue generation, productivity/performance improvement and cost-reduction. Design and implement training programs that are meaningful to your workforce and at a minimum emphasize to each member exactly what they should do if something seems to be going wrong. Use situations in which something goes wrong as teachable moments. Finally, take the time to write readily digestible policies, procedures and work instructions and locate them centrally so that your workforce can review them when relevant and apply them to situations as they occur.

**4. Design and Conduct a Risk Assessment**. Whether you choose to use one of the countless tools or templates readily available or engage an expert to come in and assist you, develop a strategy for evaluating how close or far your current operations and controls are from where you need to be to assure your confidential information is well protected and is available when you need it. Many experts feel what gets measured gets done – so develop benchmarks and use standards and

specifications to continually assess and improve on your privacy and data security compliance efforts. Each time an incident occurs, reflect on past risk assessments and assure that in future ones you zero in on lessons learned to assure the corrective measures you put in place are effective.

**5. Put Somebody In Charge.** It is critical to identify one or a small number of people in your workforce to whom you want the remainder of your workforce to head when trouble is detected. This go-to person needs to be non-judgmental and have excellent investigative skills and a desire and commitment to keep current with the dynamic state and federal legal climate relative to privacy and data security. Your key privacy/security person (depending upon the size and complexity of your organization these do not necessarily need to be the same person) can be available to interact with your vendors' and clients' privacy officers as well as with your customers.