Solutions Law Press

HR & BENEFITS UPDATE

February 22, 2011

Health Plans & Business Associates Beware!
$4.3 Million Penalty Signals OCR Serious About HIPAA Enforcement

Stamer To Discuss Privacy Risk Management At 2/25 and 3/4 SWBA/IRS 2011 Plan Administrator Skills Workshops

A $4.3 million civil monetary penalty (CMP) imposed by the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) against Cignet Health of Prince George's County, Md., (Cignet) signals the growing need for health plans and their sponsors, health care providers, health care clearinghouses and their business associates covered by the Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule to get serious about HIPAA compliance.

The first CMP ever assessed by OCR under the HIPAA Privacy Rule, the Cignet CMP assessment announced February 22, 2011 is the latest in a series of developments documenting the rising risks that health care providers, health plans, health care clearinghouses and their business associates ("covered entities") face for violations of HIPAA. Health plans and other covered entities as well as their business associates should tighten privacy policies, breach and other monitoring, training and other practices to mitigate against exposures in light of recently tightened requirements and new enforcement risks. To minimize the potential that the health plan's sharing of information with the employer will create or spread HIPAA or other privacy risks to the employer or members of its workforce, employers and other plan sponsors and members of their workforce also should take steps to ensure not only that their health plan documents, policies and procedures, as well as those policies and practices applicable to employer, its human resources, and benefits advisors when accessing or handling health plan or other medical information on behalf of the employer, rather than the plan, are appropriately designed and administered.

$4.3 Million Cignet Civil Monetary Penalty & Other CMS Enforcement Rising

In October, 2010, OCR found Cignet violated 41 patients' HIPAA rights and committed other HIPAA violations. HIPAA Privacy Rule restricts the use, access and disclosure by covered entities of PHI and other individually identifiable health care information to those outlined within the Rules. Under HIPAA covered entities also are responsible for establishing and enforcing policies and procedures that safeguard PHI against improper use, access or disclosure by employees, business associates, and other third parties. Noncompliance with the Privacy and Security Rules exposes a covered entity to criminal prosecution and penalties, civil penalties or both. The Notice of Final Determination (Final Determination) assessing the $4.3 million CMP against Cignet announced February 22, 2011 sanctions these violations by applying the expanded HIPAA violation categories and increased HIPAA civil monetary penalty amounts authorized by HIPAA amendments made by Section 13410(d) of the Health Information Technology for Economic and Clinical Health (HITECH) Act. **Read more details about Cignet violations.**

Even before the announcement of the Cignet CMP, the HIPAA Privacy exposures of covered entities for failing to comply with HIPAA already had risen significantly. As of January 1, 2011, OCR reports that 12,781 of the cases it has investigated have been resolved by requiring changes in privacy practices and other corrective actions by the covered entities and has referred more than 484 Privacy Rule breach investigations to the Department of Justice for consideration for potential criminal prosecution. While OCR had not assessed any civil monetary penalties against any covered entity for violation of HIPAA before Cignet, OCR's collection of $1 Million from Rite Aid in a 2010 Resolution Agreement, $2.25 million from CVS Pharmacy, Inc. under a 2009 Resolution Agreement and $100,000 from Providence Health & Services under a 2008 Resolution Agreement demonstrated that covered entities could face significant civil liability for willful violations of the Privacy Rules. See e.g., **Rite Aid Pays $1 Million HIPAA Privacy Settlement As OCR Tightens HIPAA Regulations.** The Department of Justice has secured several criminal convictions or pleas under HIPAA's criminal provisions. OCR data confirms that the covered entities involved in these actions included health care providers, health plans, and others.

OCR's February 18, 2009 announcement of the CVS Resolution Agreement came just one day after President Obama signed into law the HITECH Act amendments to HIPAA that among other things, modify and expand the HIPAA audit obligations of OCR, amend and expand the potential penalties, make business associates liable for violation of the privacy rules like covered entities, require covered entities and business associates to provide notification of breaches of unsecured PHI and to tighten other HIPAA obligations, and empower state attorneys' general to bring civil lawsuits against covered entities and business associates that commit HIPAA violations that injure citizens in their state under certain circumstances. See **HIPAA Heats Up: HITECH Act Changes Take Effect & OCR Begins Posting Names, Other Details Of Unsecured PHI Breach Reports On Website.**

In addition to these HIPAA-specific exposures, wrongful use, access or disclosure of medical information also can expose Covered Entities, members of their workforce and others improperly using, accessing or disclosing protected health information to liability under other federal or state laws. Federal and state prosecutors may and increasingly do bring criminal or civil actions against organizations or individuals for improperly accessing or using medical or other personal information under a variety of other federal or state laws . See e.g., **Cybercrime & Identity Theft: Health Information Security Beyond HIPAA; NY AG Cuomo Announcement of 1st Settlement For Violation of NY Security Breach Notification Law; Woman Who Revealed AIDs Info Gets A Year.**

Act To Manage HIPAA Exposures

In response to these expanding exposures, covered entities and their business associates should review the adequacy of their current HIPAA Privacy and Security compliance policies, monitoring, training, breach notification and other practices taking into consideration the Cignet, Rite Aid, Provident and CVS enforcement actions, emerging litigation and other enforcement data.; their own and reports of other security and privacy breaches and near misses, and other developments to determine if additional steps are necessary or advisable.

To minimize the potential that the health plan's sharing of information with the employer will create or spread HIPAA or other privacy risks to the employer or members of its workforce, employers and other plan sponsors and members of their workforce also should take steps to ensure not only that their health plan documents, policies and procedures, as well as those policies and practices applicable to employer, its human resources, and benefits advisors when accessing or handling health plan or other medical information on behalf of the employer, rather than the plan, are appropriately designed and administered.

As part of this process, steps that concerned covered entities, business associates and employers should consider include:

- Reviewing the adequacy of the practices, policies and procedures of the Covered Entities, business associates, and others that may come into contact with protected health information within the scope of attorney-client privilege taking into consideration the Corrective Action Plan, published OCR noncompliance and enforcement statistics, their own and reports of other security and privacy breaches and near misses, and other developments to determine if additional steps are necessary or advisable;
- Updating policies, privacy and other notices, practices, procedures, training and other practices as needed to promote compliance and defensibility;
- Renegotiating and enhancing service provider agreements to detail the specific compliance obligations of each party; to clarify the respective rights, procedures and responsibilities of each party in regards to compliance audits, investigation, breach reporting, and mitigation; to clarify rights of indemnification; and other related relevant matters;
- Improving technological and other tracking, documentation and safeguards and controls to the use, access and disclosure of protected health information;
- Conducting well-documented training as necessary to ensure that members of the Covered Entity's workforce understand and are prepared to comply with the expanded requirements of HIPAA, can detect potential breaches or other compliance concerns, and understand and are prepared to follow appropriate procedures for reporting and responding to suspected violations;
- Tracking actual and near miss violations and making adjustments to policies, practices, training, safeguards and other compliance components as necessary to deter future concern
- Establishing and providing well-documented monitoring of compliance;
- Establishing and providing well-documented timely investigation and redress of reported violations or other compliance concerns;
- Establishing contingency plans for responding in the event of a breach;
- Establishing a well-documented process for monitoring and updating policies, practices and other efforts in response to changes in risks, practices and requirements;
- Preparing and maintaining a well-documented record of compliance activities; and
- Pursuing other appropriate strategies to enhance the Covered Entity's ability to demonstrate its compliance commitment both on paper and in operation.

For Help With Investigations, Policy Review & Updates Or Other Needs

If you need assistance in auditing or assessing, updating or defending your HIPAA or other health plan, or other labor and employment, employee benefit, compensation, privacy and data security, or other internal controls and practices, please contact the author of this update, attorney Cynthia Marcotte Stamer **here** or at (469)767-8872.

Ms. Stamer, a noted Texas-based employee benefits and employment lawyer Board Certified in Labor & Employment Law by the Texas Board of Legal Specialization, will discuss HIPAA and other privacy risks and risk management strategies for employers, health and employee benefit plan sponsors and their administrators at the Southwest Benefits Association/IRS Plan Administrator Skills Workshops to be held February 25 in Dallas and March 4 in Houston.

The Chair of the American Bar Association (ABA) RPTE Employee Benefits & Other Compensation Committee, a Council Representative on the ABA Joint Committee on Employee Benefits, Government Affairs Committee Legislative Chair for the Dallas Human Resources Management Association, and past Chair of the ABA Health Law Section Managed Care & Insurance Interest Group, Ms. Stamer works, publishes and speaks extensively on HIPAA and other privacy and data security, health plan, health care and other human resources and workforce, employee benefits, compensation, internal controls and related matters.

For more than 23 years, Ms. Stamer has counseled, represented and trained employers and other employee benefit plan sponsors, plan administrators and fiduciaries, insurers and financial services providers, third party administrators, human resources and employee benefit information technology vendors and others privacy and data security, fiduciary responsibility, plan design and administration and other compliance, risk management and operations matters. She also is recognized for her publications, industry leadership, workshops and presentations on privacy and data security and other human resources, employee benefits and health care concerns. Her many highly regarded publications on privacy and data security concerns include *"Privacy Invasions of Medical Care-An Emerging Perspective."* ERISA Litigation Manual. BNA, 2003-2009; *"Privacy & Securities Standards-A Brief Nutshell."* BNA Tax Management and Compliance Journal. February 4, 2005; *"Cybercrime and Identity Theft: Health Information Security beyond HIPAA."* ABA Health eSource. May, 2005 and many others. She also regularly conducts training

on HIPAA and other privacy and data security compliance and other risk management matters for a broad range of organizations including the Association of State and Territorial Healthcare Organizations (ASTHO), the Los Angeles County Health Department, a multitude of health plans and their sponsors, health care providers, the American Bar Association, SHRM, the Society for Professional Benefits Administrators and many others.t Her insights on these and other matters appear in the Bureau of National Affairs, Spencer Publications, the Wall Street Journal, the Dallas Business Journal, the Houston Business Journal, and many other national and local publications. For additional information about Ms. Stamer and her experience or to access other publications by Ms. Stamer see **here** or contact Ms. Stamer directly.

About Solutions Law Press

Solutions Law Press™ provides business risk management, legal compliance, management effectiveness and other resources, training and education on human resources, employee benefits, data security and privacy, insurance, health care and other key compliance, risk management, internal controls and operational concerns. If you find this of interest, you also be interested reviewing some of our other Solutions Law Press resources including:

- **ERISA Leader Nell Hennessy Dies From Cancer**
- **IRS Expands When HFSAs & HRAS May Allow Over-The-Counter Drug Purchases With Drug Cards**
- **IRS, HHS & DOL To Delay Enforcement of New Insured Group Health Plan Non-Discrimination Rules Pending Guidance; Seek Public Input on Rules**
- **DOL Announces Changes To H-2B Prevailing Wage Calculation Rules**
- **$1 Million + FLSA Overtime Settlement Shows Employers Should Tighten On-Call, Other Wage & Hour Practices**
- **Medical Resident Stipend Ruling Shows Health Care, Other Employers Should Review Worker Classification, Payroll & Other Practices**
- **CMS Physician Compare Web Site Offers Consumers New Provider Info Source**
- **Holiday Season Celebration Reminder To Manage Intoxication Risks**
- **Avoiding Post-Holiday Celebration Sexual Harassment & Discrimination Liability**
- **Small Employers Should Weigh If Health Premium Tax Credit Justifies Changing Employee Leasing Arrangements**
- **2011 Standard Mileage Rates Announced**
- **Free 12/6/10 ABA RPTE Employee Benefit Groups Study Group Conference Call Examines PBGC Enforcement of Downsizing Liability, Updated Reporting & Other PBGC Developments**
- **Proposed New Defined Benefit Plan Annual Funding Notice Rule Reminder of Need to Carefully Manage Pension Plan Responsibilities**
- **Affordable Care Act Grandfathered Plan Rules Loosened To Allow Insured Plans Making Some Insurance Changes To Qualify**
- **Update Employment Practices To Manage Genetic Info Discrimination Risks Under New EEOC Final GINA Regulations**
- **EEOC Attacks Medical Leave Denials As Prohibited Disability Discrimination**
- **DOL Proposes To Expand Investment Related Services Giving Rise to ERISA Fiduciary Status As Investment Fiduciary**

If you or someone else you know would like to receive future updates about developments on these and other concerns, please be sure that we have your current contact information – including your preferred e-mail – by creating or updating your profile at **here** or e-mailing this information **here**. To unsubscribe, e-mail **here.**