Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

WSGR ALERT

MARCH 2012

# $1.5 MILLION SETTLEMENT AFTER HIPAA SECURITY INCIDENT RESULTS IN MORE THAN $17 MILLION IN INVESTIGATION AND REMEDIATION COSTS

## *Employer Group Health Plans, Health IT Companies, and Others Face Real Risks of Dramatic Compliance Expenses and Exposure*

Earlier this month, the Department of Health and Human Services (HHS) entered into a $1.5 million settlement[1] with BlueCross BlueShield of Tennessee to settle healthcare information privacy and security violations under the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). BlueCross had self-reported the underlying incident under HIPAA's requirements, and incurred more than $17 million in direct expenses relating to its investigation and remediation of the incident. The HHS investigators faulted BlueCross BlueShield for failing to implement appropriate administrative safeguards to protect information by storing protected health information on unencrypted computer hard drives. Under the settlement, BlueCross BlueShield also agreed to review and revise its healthcare information privacy and security policies, and to train employees regularly for HIPAA compliance.

This settlement represents a continuing trend of dramatically increased HIPAA enforcement activity with escalating fines, dramatic increases in investigatory and remediation expenses, and parallel enforcement by states. The BlueCross matter is equally significant because it is the first settlement resulting from the notification of a security incident to HHS under its breach-notification rules.

### Why Should Employers Be Concerned?

For employers (and service providers that support entities covered by HIPAA as business associates), this development is significant because it shows that the healthcare system, which is driven largely by employer-sponsored plans, has become a significant priority for regulators, including with regard to healthcare privacy and data security. In addition, a number of new laws and regulations that trigger additional risks have emerged for group health plans in recent years. The new emphasis by regulators on the healthcare system has broadened the scope of legal obligations for most employers, and it dramatically has increased penalties for noncompliance. As HHS and the other state and federal agencies pursue legal action, employers undoubtedly will become targets for oversight and enforcement.

The remainder of this WSGR Alert focuses upon risks to employers operating health plans. HIPAA triggers important additional obligations for many other types of businesses, and this latest enforcement action highlights these risks.

In the current regulatory and enforcement environment, we recommend that employers obtain a better understanding of the rules applicable to their group health plans by reviewing their legal obligations and risks.

### Common Health Plan Activities Calling for Legal Attention

Employers that sponsor self-funded medical and prescription drug plans often are aware of the substantial cost and administration necessary for legal compliance under those plans. Employers with self-funded plans should take note that there have been several multimillion-dollar HHS enforcement actions in the last 12 months, and they should consider what steps to take if a HIPAA or other healthcare-related audit occurs.

Importantly, employers that do not offer self-funded medical or prescription drug plans can still trigger material obligations and risk under the new structure of the healthcare laws. The following, lesser-known activities have been affected by recent healthcare laws and should be reviewed for legal compliance with HIPAA, GINA,[2] ERISA,[3] ADA,[4] COBRA,[5] tax laws, and other employment laws. These activities should be coordinated with health

[1] To learn more about the settlement, please visit http://www.hhs.gov/news/press/2012pres/03/20120313a.html.

[2] Genetic Information Nondiscrimination Act of 2008, as amended (GINA).

[3] Employee Retirement Income Security Act of 1974, as amended (ERISA).

[4] American with Disabilities Act of 1990, as amended (ADA).

[5] Title X of the Consolidated Omnibus Budget Reconciliation Act of 1985, as amended (COBRA).

*Continued on page 2...*

## *$1.5 Million Settlement after HIPAA Security Incident . . .*

*Continued from page 1...*

insurance policies and/or third-party administration agreements as well:

- Managing a "wellness program," in whole or in part, within the human resources department
- Imposing restrictions or providing rewards to employees based on employee lifestyle choices (e.g., smoking cessation, gym attendance, Weight Watchers, and other "healthiness" cash or gift reward programs) in a health plan or through a company policy
- Self-funding a vision, dental, or employee assistance program
- Self-administering health flexible spending, dependent care assistance, or healthcare reimbursement accounts, or other health plans
- Extending to former employees health plan coverage that is not related to COBRA coverage
- Providing group health plan coverage to employees on a discriminatory basis
- Paying for or reimbursing a former employee for health plan premiums
- Assisting employees with submitting or appealing healthcare claims
- Establishing an on-site medical treatment program

**Recent Developments in Enforcement**

Employers should be aware that regulators have taken a number of notable steps toward enforcement, armed with a cache of civil penalties built into the new healthcare laws and regulations. For example, below is a brief timeline of recent laws, regulations, and policies established by various federal agencies since early 2009, all of which increase government oversight and enforcement:

- *February 17, 2009*: The TARP[6] law features sweeping changes related to health information privacy under HIPAA by extending the reach of HIPAA penalties, requiring self-reporting of health information privacy violations to HHS, and significantly increasing civil penalties for violations.
- *September 8, 2009*: The Internal Revenue Service (IRS) issues final regulations on paying excise taxes for various group health plan violations (e.g., failure to comply with COBRA, HIPAA, mental health parity rules, GINA, provision of health benefits to adult minors, or health savings account contribution rules). If employers fail to self-report violations under the tax laws, excise taxes arise in the year of violation (in addition to other civil penalties that may be levied by other federal and state agencies). If excise taxes are not self-reported on a timely basis, another layer of tax penalties under the tax laws can apply. This self-reporting obligation is a dramatic departure from the prior IRS position of non-enforcement on audit.
- *March 23, 2010*: Health reform laws reorganize the nation's private and employer-driven healthcare system, including the addition of new rules and regulations with effective dates ranging from 2011 through 2018. These laws impose multiple penalties and taxes for non-compliance with various healthcare mandates. For example, one portion of the health reform law imposes significant excise taxes on certain employers with insured group health plans that discriminate in favor of highly compensated individuals. This law likely limits the typical practice of providing employees with reimbursement of COBRA premiums after terminations, layoffs or other reductions in force. The excise tax is $100 per day during the period of noncompliance with respect to each individual to whom the failure relates, but not to exceed the lesser of either 10 percent of the group health plan costs or $500,000. In IRS Notice 2010-63, the IRS indicated that the individuals "to whom the failure relates" are those employees who are discriminated against (not the individual(s) receiving the discriminatory benefit)—typically a large group of employees.
- *November 2011*: HHS begins a random audit pilot program of entities for HIPAA compliance, including business associates of entities covered by HIPAA. This audit program is intended to be a model for future HHS action.

**Lessons Employers Can Take Away**

In our review of these new laws and regulations for group health plans, as well as our observance of the tone taken by regulators, we believe it is important for employers to take away the following lessons from the strong current of healthcare oversight and enforcement:

- Innocent mistakes nevertheless may result in substantial penalties or settlements.
- Relying on outside vendors or other third parties does not insulate an employer from liability. A careful review of indemnification and limitation-of-liability provisions in contracts with these parties likely is warranted.
- Failure by an outside vendor or insurer to comply with healthcare laws can result in significant tax penalties for an employer.
- Companies inadvertently can cause significant tax liabilities for employees and former employees by not observing healthcare nondiscrimination rules.
- For large employers with self-funded group health plans, the imposition of civil

[6]Title XIII of American Recovery and Reinvestment Act of 2009 (ARRA) is known as the Health Information Technology for Economic and Clinical Health Act (the HITECH Act).

*Continued on page 3...*

## *$1.5 Million Settlement after HIPAA Security Incident . . .*

*Continued from page 2...*

penalties under HIPAA should be viewed as a potentially significant and adverse development.

- Companies with employees who handle any protected health information should review their HIPAA privacy and security policies and procedures. They should implement such policies and procedures as necessary, and provide appropriate training. Training should be well-documented and updated as necessary for new legal requirements and evolving best practices.

This WSGR Alert is intended only as a general summary. If you have any questions regarding this alert, please contact any member of the employee benefits and compensation practice of Wilson Sonsini Goodrich & Rosati:


| | |
|---|---|
| John Aguirre | (650) 565-3603 |
| Melody Barker | (415) 947-2029 |
| Ralph Barry | (858) 350-2344 |
| Jessica Bliss | (650) 849-3470 |
| Madeleine Boshart | (415) 947-2057 |
| Mark Cornillez-Ty | (650) 849-3384 |
| Stephen Francis | (650) 849-3381 |
| Brandon Gantus | (415) 947-2138 |
| Michael Klippert | (650) 849-3276 |
| Sriram Krishnamurthy | (650) 849-3309 |
| Scott McCall | (650) 320-4547 |
| Michael Montfort | (202) 973-8815 |
| Cisco Palao-Ricketts | (650) 565-3617 |
| Christa Sanchez | (650) 849-3382 |
| Roger Stern | (650) 320-4818 |
| David Thomas | (650) 849-3261 |
| Michelle Wallin | (650) 565-3620 |


If you have any other privacy or data security questions related to HIPAA, please contact a member of our Privacy and Data Security practice.

**Circular 230 Compliance: To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained in this Alert is not intended or written to be used, and cannot be used, for the purpose of (a) avoiding penalties under the U.S. Internal Revenue Code, or (b) promoting, marketing, or recommending to another party any transaction or matter addressed herein.**


WSGR

Wilson Sonsini Goodrich & Rosati

PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on March 26, 2012. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.





650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com