

# The Advocate

Official Publication  
of the Idaho State Bar  
Volume 55, No. 6/7  
June/July 2012

Sponsored by the  
Health Law Section



# BEWARE HIPAA'S NEW PENALTIES: WHAT YOU AND YOUR CLIENTS SHOULD KNOW

Kim C. Stanger  
Holland & Hart, LLP

Recent changes to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security rules dramatically increase attorneys' and their clients' potential liability for HIPAA violations.

## HIPAA now applies directly to some attorneys

The HIPAA privacy and security rules apply to "covered entities," which includes most health care providers, health care clearinghouses, health insurers, and employee group plans that have 50 or more participants or that are administered by a third party. Effective February 2010, HIPAA also applies directly to "business associates" of covered entities, which includes attorneys who (1) represent a covered entity or a covered entity's business associate, and (2) receive protected health information from the client or the client's business associate in the course of representing the client. "Protected health information" is individually identifiable information about a person's health, health care, or payment for his or her health care. The net result is that attorneys who are business associates of covered entities and larger law firms' group health plans, must comply with most HIPAA requirements or face increased HIPAA penalties.

## Must self-report HIPAA breaches

Effective February 2010, covered entities and business associates must self-report HIPAA violations that pose a significant risk of financial, reputational or other harm to the individual whose information was breached. If the business associate learns of such a breach, it must report the breach to the covered entity without unreasonable delay. The covered entity must report a breach to the affected individual or his or her personal representatives and the federal Department of Health and Human Services (HHS). If the breach involves more than 500 per-



Kim C. Stanger

sons, the covered entity must also report information about the breach through local media. Needless to say, the self-reporting requirement increases the potential for HIPAA penalties.

## HIPAA civil penalties are now mandatory

In 2009, the penalties for HIPAA violations were increased 500 times the prior amount. To make matters worse, effective February 2011, the Office of Civil Rights ("OCR") is required to impose HIPAA penalties if the covered entity or business associate acted with willful neglect, i.e., "the conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA requirements. The new penalty structure is as follows:

Conduct of Covered Entity or Business Associate	Penalty
Did not know and, by exercising reasonable diligence, would not have known of the violation.	\$100 to \$50,000 per violation; Up to \$1,500,000 per identical violation per year.
Violation due to reasonable cause and not willful neglect.	\$1,000 to \$50,000 per violation; Up to \$1,500,000 per identical violation per year.
Violation due to willful neglect but the violation is corrected within 30 days after the covered entity knew or should have known of the violation.	Mandatory fine of \$10,000 to \$50,000 per violation; Up to \$1,500,000 per identical violation per year.
Violation due to willful neglect and the violation was not corrected within 30 days after the covered entity knew or should have known of the violation.	Mandatory fine of not less than \$50,000 per violation; Up to \$1,500,000 per identical violation per year.

*In 2009, the penalties for HIPAA violations were increased 500 times the prior amount.*

The government is serious about the new penalties: the OCR has imposed millions of dollars in penalties or settlements since the mandatory penalties took effect. Recent HIPAA amendments also authorize state attorneys general to sue individuals for HIPAA violations and recover penalties in the amount of \$25,000 per violation plus fees. The amendments also permit affected individuals to recover a portion of any settlement or penalties related to a HIPAA violation, thereby increasing their incentive to report HIPAA violations. Regulations implementing the amendments are pending.

The good news is that if the covered entity or business associate does not act with willful neglect, the OCR may waive or reduce the penalties, depending on the circumstances of the violation. More importantly, if the covered entity or business associate does not act with willful neglect and corrects the violation within 30 days, the OCR may not impose any penalty; timely correction constitutes an affirmative defense.

## HIPAA violations may be a crime

Even if not a business associate, attorneys and any other individuals may be liable under HIPAA's criminal statute for improperly obtaining or disclosing protected health information from a covered entity without authorization:

Prohibited Conduct	Penalty
Knowingly obtaining or disclosing protected health information without authorization.	Up to \$50,000 fine and one year in prison.
If done under false pretenses.	Up to \$100,000 fine and five years in prison.
If done with intent to sell, transfer, or use the information for commercial advantage, personal gain or malicious harm.	Up to \$250,000 fine and ten years in prison.



## What your clients (and you) need to do to avoid penalties.

Given this increased exposure, covered entities and their attorneys need to do the following to avoid HIPAA penalties:

**1. Read the rules.** There is no substitute for actually knowing the rules, which are found at 45 C.F.R. part 164. The OCR maintains a very helpful website to facilitate HIPAA compliance: [www.hhs.gov/ocr/privacy](http://www.hhs.gov/ocr/privacy). Among other things, the website contains copies and summaries of the rules, guides, forms, and frequently asked questions.

**2. Assign HIPAA responsibility.** Covered entities must designate persons to serve as HIPAA privacy and security officers and document the designation in writing. The privacy and security officers are responsible for ensuring HIPAA compliance.

**3. Comply with use and disclosure rules.** The basic privacy rules are simple. In general, covered entities and business associates may not use, access or disclose protected health information without the patient's valid, HIPAA-compliant authorization unless the use or disclosure fits within an exception. Covered entities and business associates may use or disclose protected health information for purposes of treatment, payment or certain health care operations without the patient's consent. However, they may not use or disclose more than is minimally necessary for the permitted purpose.

**4. Comply with patient rights.** HIPAA grants patients certain rights concerning their health information. Among others, patients generally have a right to obtain copies of their protected health information, request amendment to their information, and obtain an accounting of impermissible disclosures. Covered entities and business associates must allow patients to exercise their rights. Cignet Health was fined \$4.3 million for, among other things, failing to timely respond to patient requests to access their health information.

**5. Maintain written policies.** HIPAA requires covered entities and business associates to develop and maintain written policies that implement the privacy and security rule requirements. Having the required policies is a key to avoiding penalties: it may be difficult to avoid a finding of willful neglect if you failed to implement the policies required by HIPAA. HHS has indicated that maintaining the

*If the breach involves less than 500 persons, the covered entity must notify HHS by filing an electronic report no later than 60 days after the end of the calendar year.*

required written policies is a significant factor in avoiding penalties imposed for "willful neglect." In contrast, Rite Aid paid \$1 million to settle HIPAA violations based on its failure to maintain required HIPAA policies.

**6. Develop compliant forms.** HIPAA requires that certain documents used by covered entities and business associates satisfy regulatory requirements. For example, HIPAA authorizations must contain certain elements to be valid. Covered entities must provide patients with a notice of privacy practices that contains certain statements. Other forms may be developed to ensure compliance with patient rights. Ensure your HIPAA forms satisfy the regulatory requirements.

**7. Execute business associate agreements.** Although HIPAA now applies directly to business associates, HIPAA still requires covered entities to execute "business associate agreements" with their business associates before disclosing protected health information to the business associate. Under proposed rules, attorneys and other business associates must execute similar agreements with subcontractors to whom the business associate discloses protected health information. The business associate agreements must contain certain elements. Breach of the business associate agreement exposes the business associate to contract claims by the covered entity in addition to the civil or criminal penalties that may follow HIPAA violations.

**8. Train employees and agents.** Having the policies and forms is only the first step. Covered entities and business associates must train their agents to comply with the policies and agreements. HIPAA requires that new employees be trained within a reasonable period of time upon hire, and as needed thereafter. Documented training is a second most important step to avoid HIPAA compliance. In commentary to HIPAA's new penalties, HHS indicated that covered entities may

avoid HIPAA penalties based on the misconduct of a rogue employee so long as the covered entity implemented appropriate policies and adequately trained the employee.

**9. Use appropriate safeguards.** The government recognizes that patient information cannot be absolutely protected; accordingly, HIPAA does not impose liability for "incidental disclosures" so long as the covered entity or business associate implemented reasonable administrative, technical, and physical safeguards designed to protect against improper disclosures. The security rule contains detailed regulations concerning safeguards that must be implemented to protect electronic health information. The privacy rule is less specific. Reasonable safeguards may include, e.g., not leaving protected health information where it may be lost or improperly accessed; checking e-mail addresses and fax numbers before sending using fax cover sheets; etc.

**10. Respond immediately to any breach.** This is critical for several reasons. First, HIPAA requires covered entities and business associates to investigate any privacy complaints, mitigate any breach, and impose appropriate sanctions against any agent who violates HIPAA. It may also require covered entities to terminate an agreement with a business associate due to the business associate's noncompliance. Second, an entity may be able to ameliorate or negate any risk of harm to the affected individual by taking swift action, thereby avoiding the obligation to self-report HIPAA violations to the individual and the government. Third, a covered entity or business associate can avoid HIPAA penalties altogether if it corrects the violation within 30 days.

**11. Timely report breaches.** If a breach of unsecured protected health information poses a risk of significant financial, reputational or other harm to the individual, business associates must promptly report the breach to covered entities, and cov-

ered entities must notify the individual within 60 days. If the breach involves less than 500 persons, the covered entity must notify HHS by filing an electronic report no later than 60 days after the end of the calendar year. If the breach involves 500 or more persons, the covered entity must file the electronic report at the same time it gives notice to the individual. The written notice to the individual must satisfy certain regulatory requirements.

**12. Document your actions.** Documentation of proper action is essential to defend yourself against HIPAA claims. In addition, covered entities and business associates are generally required to maintain documentation required by HIPAA for six years.

**13. Watch for new rules.** As I write this article, the Office of Management and Budget is considering new HIPAA regulations, including those affecting business associate responsibilities. Attorneys and their health care clients should watch for the new regulations and implement any additional changes as necessary.

#### About the Author

**Kim C. Stanger** is a partner at *Holland & Hart, LLP* in Boise. Mr. Stanger

*handles simple and complex healthcare transactions, including practitioner and payor contracts; joint ventures; practice formations, acquisitions, and mergers; conversions; and physician integration. He helps clients comply with numerous laws and regulations governing healthcare, including Stark, the Anti-Kickback Statute, HIPAA, EMTALA, HITECH, Medicare and Medicaid requirements, and licensing rules.*

#### Endnotes

- <sup>1</sup> "HIPAA" is the Health Insurance Portability and Accountability Act. The HIPAA privacy and security rules are found at 45 C.F.R. part 164.
- <sup>2</sup> 45 C.F.R. § 160.103 (definition of *covered entity*).
- <sup>3</sup> *Id.* (definition of *business associate*).
- <sup>4</sup> *Id.* (definition of *protected health information*).
- <sup>5</sup> 45 C.F.R. § 164.400 *et seq.*
- <sup>6</sup> 45 C.F.R. § 164.410.
- <sup>7</sup> 45 C.F.R. §§ 164.404 and .408.
- <sup>8</sup> 45 C.F.R. §§ 164.406.
- <sup>9</sup> 45 C.F.R. §§ 160.404.
- <sup>10</sup> 45 C.F.R. §§ 160.401 and .404; *see* 75 F.R. 40876.
- <sup>11</sup> *See, e.g.,* reported enforcement actions listed at <http://www.hhs.gov/ocr/privacy> (last visited April 26, 2012).
- <sup>12</sup> 42 U.S.C. § 1320d-5(d).
- <sup>13</sup> 45 C.F.R. § 160.408.
- <sup>14</sup> 45 C.F.R. § 160.410.
- <sup>15</sup> 42 U.S.C. § 1320d-6.
- <sup>16</sup> 45 C.F.R. § 164.530(a).
- <sup>17</sup> 45 C.F.R. § 164.502(a).
- <sup>18</sup> 45 C.F.R. § 164.502(b).

- <sup>19</sup> 45 C.F.R. § 164.524.
- <sup>20</sup> 45 C.F.R. § 164.526.
- <sup>21</sup> 45 C.F.R. § 164.528.
- <sup>22</sup> *See* <http://www.hhs.gov/news/press/2011pres/02/20110222a.html> (last visited April 26, 2012).
- <sup>23</sup> 45 C.F.R. § 164.316(a) and .530(f).
- <sup>24</sup> *See* 75 F.R. 48078-79.
- <sup>25</sup> *See* <http://www.hhs.gov/news/press/2010pres/07/20100727a.html> (last visited April 26, 2012).
- <sup>26</sup> 45 C.F.R. § 164.508.
- <sup>27</sup> 45 C.F.R. § 164.520.
- <sup>28</sup> 45 C.F.R. § 164.308(b) and .502(e).
- <sup>29</sup> 75 F.R. 40873.
- <sup>30</sup> 45 C.F.R. § 164.314(a) and .504(e).
- <sup>31</sup> 45 C.F.R. § 164.530(b).
- <sup>32</sup> 75 F.R. 40879.
- <sup>33</sup> 45 C.F.R. § 164.502(a)(1)(iii); *see* OCR Guidance on Significant Aspects of the Privacy Rule: Incidental Uses and Disclosures, available at: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalsusesanddisclosures.html> (last visited April 26, 2012).
- <sup>34</sup> 45 C.F.R. § 164.308-.316, and Appendix A to 45 C.F.R. subpart C of part 164.
- <sup>35</sup> 45 C.F.R. § 164.530(c).
- <sup>36</sup> 45 C.F.R. § 164.530(d)-(f).
- <sup>37</sup> *See* 45 C.F.R. § 164.314(a)(2)(i)(D) and .504(e)(2)(iii).
- <sup>38</sup> *See* 74 F.R. 42744-45.
- <sup>39</sup> 45 C.F.R. § 160.410.
- <sup>40</sup> 45 C.F.R. §§ 164.404-.410.
- <sup>41</sup> 45 C.F.R. § 164.408(c).
- <sup>42</sup> 45 C.F.R. § 164.408(b).
- <sup>43</sup> 45 C.F.R. § 164.404.
- <sup>44</sup> 45 C.F.R. § 164.530(j).



**THE James Street GROUP**  
Settlement Planners

**Planning.  
Protection.  
Peace of Mind.**

Structured Settlements  
Structured Attorney Fees  
Government Benefit Protection  
Trust Services  
Lien Resolution Services  
Medicare Set-Asides (MSAs)

*Comprehensive settlement planning for you and your client.*



**Audrey Kenney**  
[akenney@tjsg.com](mailto:akenney@tjsg.com)  
 (208) 631-7298  
[www.tjsg.com](http://www.tjsg.com)

## Huegli

### Mediation & Arbitration


*Serving Idaho, Oregon and Washington*

**Personal injury, commercial disputes,  
construction law, professional liability.**

**Available Statewide.**

*39 years litigation experience.*

*Martindale-Hubbell AV Rated.*



**James D. Huegli**  
 1770 West State Street, Suite 267  
 Boise, ID 83702  
**Phone:** (208) 631-2947  
**Fax:** (208) 629-0462  
**Email:** [jameshuegli@yahoo.com](mailto:jameshuegli@yahoo.com)  
**Web:** [www.hueglimediation.com](http://www.hueglimediation.com)