Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Avoid New HIPAA Penalties

Avoid New HIPAA Penalties

Insight — 4/25/2012

Recent changes to the HIPAA privacy and security rules[1] dramatically increase health care providers' and their business associates' potential liability for HIPAA violations.

HIPAA Civil Penalties Are Now Mandatory. In 2009, the penalties for HIPAA violations were increased 500 times their prior limits.[2] Effective February 2011, the Office of Civil Rights ("OCR") is required to impose HIPAA penalties if the covered entity or its business associate acted with willful neglect, *i.e.*, with "conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA requirements.[3] The following chart summarizes the penalty structure:

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

The federal government is serious about the new penalties: the OCR has imposed millions of dollars in penalties or settlements since the mandatory penalties took effect.[4] State attorneys general may also sue for HIPAA violations and recover penalties of $25,000 per violation plus attorneys' fees.[5] When implemented, HITECH amendments will allow patients to recover a portion of any settlement or penalties related to a HIPAA violation, thereby increasing patients' incentive to report HIPAA violations.

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.[6] 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 is an affirmative defense.[7]

HIPAA Violations May Be A Crime. Federal law prohibits any individual from improperly obtaining or disclosing protected health information from a covered entity without authorization[8] ; violations may result in the following criminal penalties:

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

Physicians, hospital staff members, and others have been prosecuted for improperly accessing, using or disclosing protected health information.

Entities Must Self-Report HIPAA Breaches. The risk of penalties is compounded by the fact that covered entities and business associates must self-report HIPAA breaches that pose a significant risk of financial, reputational or other harm to the individual whose information was breached.[9] If the business associate learns of such a breach, it must report the breach to the covered entity without unreasonable delay.[10] The covered entity must report a breach to the affected individual or their personal representatives and the federal Department of Health and Human Services ("HHS").[11] If the breach involves more than 500 persons, the covered entity must also publish information about the breach through local media.[12]

What You Need To Do To Avoid Penalties. Given this increased exposure, health care providers and their business associates should do the following to avoid HIPAA penalties:

1. Assign HIPAA responsibility. Covered entities must designate persons to serve as their HIPAA privacy and security officers, and document the designation in writing.[13] The privacy and security officers are responsible for ensuring HIPAA compliance.

2. Know the use and disclosure rules. The basic privacy rules are simple: 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.[14] 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.[15] Additional exceptions apply to specific situations. The OCR maintains a very helpful website to aid covered entities' compliance: http://www.hhs.gov/ocr/privacy/.

3. Know patients' 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[16]; request amendment to their information[17]; and obtain an accounting of impermissible disclosures[18]. Covered entities and business associates must know and 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.[19]

4. Maintain written policies. HIPAA requires covered entities and business associates to develop and maintain written policies that implement the privacy and security rule requirements, including those dealing with confidentiality and patients' rights.[20] Having the required policies is key to avoiding penalties. According to HHS, maintaining the required written policies is a significant factor in avoiding penalties imposed for "willful neglect."[21] Rite Aid paid $1,000,000 to settle HIPAA violations based in part on its failure to maintain required HIPAA policies.[22] This week, a Phoenix cardiology group was fined $100,000 in part because it failed to have written policies required by HIPAA.[23] To obtain a checklist of required policies, contact me at kcstanger@hollandhart.com.

5. 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.[24] Covered entities must provide patients with a notice of privacy practices that contains certain statements.[25] Other forms may be developed to ensure compliance with patient rights. Ensure your HIPAA forms satisfy the regulatory requirements.

6. 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.[26] Under proposed rules, business associates must execute similar agreements with subcontractors to whom the business associate discloses protected health information.[27] The business associate agreements must contain certain elements.[28] Breach of the business associate agreement exposes the business associate to contract claims by the covered entity in addition to civil or criminal penalties imposed by the government. Covered entities are generally not liable for the actions of their business associates unless the business associate is acting as the agent of the covered entity. Make sure your business associate agreements confirm that the business associate is an independent

contractor, not your agent.

7. Train employees and agents. Having the policies and forms is only the first step; covered entities and business associates must train their employees to comply with the policies and document the training. HIPAA requires that new employees are trained within a reasonable period of time after hire, and as needed thereafter.[29] Documented training is a second critical step to avoid HIPAA penalties. According to HHS commentary, 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.[30]

8. Use appropriate safeguards. The government recognizes that patient privacy cannot be absolutely protected. 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.[31] The security rule contains detailed regulations concerning safeguards that must be implemented to protect electronic health information.[32] The privacy rule is less specific.[33] The reasonableness of safeguards depends on the circumstances, but 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 messages; using fax cover sheets; etc.

9. 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.[34] It may also require covered entities to terminate an agreement with a business associate due to the business associate's noncompliance.[35] Second, an entity may be able to ameliorate or negate any risk of harm to the patient by taking swift action, thereby avoiding the obligation to self-report HIPAA violations to the individual and HHS.[36] Third, a covered entity or business associate can avoid HIPAA penalties altogether if it does not act with willful neglect and corrects the violation within 30 days.[37]

10. Timely report breaches. If a breach of unsecured protected health information poses a risk of significant financial, reputational or other harm to the patient, business associates must promptly report the breach to covered entities, and covered entities must notify the patient within 60 days.[38] 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.[39] If the breach involves 500 or more persons, the covered entity must file the electronic report when it notifies the patient.[40] The written notice to the patient must satisfy regulatory requirements.[41]

11. Document your actions. Documenting proper actions will help you defend against HIPAA claims. Covered entities and business associates are required to maintain documentation required by HIPAA for six years.[42]

As I write this article, the Office of Management and Budget is reviewing

new HIPAA regulations. Covered entities and business associates should watch for the new regulations and implement any additional changes as necessary.

For More Information Contact:
Kim C. Stanger
Phone: 208-383-3913
Email: kcstanger@hollandhart.com

---

[1]"HIPAA" is the Health Insurance Portability and Accountability Act. The HIPAA privacy and security rules are found at 45 C.F.R. part 164.
[2]45 C.F.R. §§ 160.404.
[3]45 C.F.R. §§ 160.401 and .404; see 75 F.R. 40876.
[4]See, e.g., reported enforcement actions listed at http://www.hhs.gov/ocr/privacy.
[5]42 U.S.C. § 1320d-5(d).
[6]45 C.F.R. § 160.308(a)(2) and .408.
[7]45 C.F.R. § 160.410.
[8]42 U.S.C. § 1320d-6.
[9]45 C.F.R. § 164.400 et seq.
[10]45 C.F.R. § 164.410.
[11]45 C.F.R. §§ 164.404 and .408.
[12]45 C.F.R. §§ 164.406.
[13]45 C.F.R. § 164.530(a).
[14]45 C.F.R. § 164.502(a).
[15]45 C.F.R. § 164.502(b).
[16]45 C.F.R. § 164.524.
[17]45 C.F.R. § 164.526.
[18]45 C.F.R. § 164.528.
[19]See http://www.hhs.gov/news/press/2011pres/02/20110222a.html.
[20]45 C.F.R. § 164.316(a) and .530(f).
[21]See 75 F.R. 48078-79.
[22]See http://www.hhs.gov/news/press/2010pres/07/20100727a.html.
[23]See http://www.hhs.gov/news/press/2012pres/04/20120417a.html.
[24]45 C.F.R. § 164.508.
[25]45 C.F.R. § 164.520.
[26]45 C.F.R. § 164.308(b) and .502(e).
[27]75 F.R. 40873.
[28]45 C.F.R. § 164.314(a) and .504(e).
[29]45 C.F.R. § 164.530(b).
[30]75 F.R. 40879.
[31]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://1.usa.gov/4FWXU6.
[32]45 C.F.R. § 164.308-.316, and Appendix A to 45 C.F.R. subpart C of part 164.
[33]45 C.F.R. § 164.530(c).
[34]45 C.F.R. § 164.530(d)-(f).
[35]See 45 C.F.R. § 164.314(a)(2)(i)(D) and .504(e)(2)(iii).
[36]See 74 F.R. 42744-45.
[37]45 C.F.R. § 160.410.
[38]45 C.F.R. §§ 164.404-.410.
[39]45 C.F.R. § 164.408(c).
[40] 45 C.F.R. § 164.408(b).
[41]45 C.F.R. § 164.404.

[42]45 C.F.R. § 164.530(j).

Subscribe to get our Insights delivered to your inbox.