February 2010 Newsletter

HIPAA Penalties for Noncompliance—UPDATE

HIPAA's enforcement provisions authorize the Secretary to impose penalties to non-complying entities. The HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009, addresses privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Eliminated was the exception to the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (such violations are now punishable under the lowest tier of penalties); and provided is a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect. This interim final rule was effective on November 30, 2009.

Civil Penalties

Following are the categories of violations and associated penalty amounts available.

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Such Violations of an Identical Provision in a Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100-50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000-50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Corrected</td>
<td>$10,000-50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

Federal Criminal Penalties

Covered entities and specified individuals, as explained below, whom "knowingly" obtain or disclose individually identifiable health information in violation of the Administrative Simplification Regulations face a fine of up to $50,000, as well as imprisonment up to one year.

Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison.

Finally, offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

Covered Entity and Specified Individuals

The DOJ concluded that the criminal penalties for a violation of HIPAA are directly applicable to covered entities—including health plans, health care clearinghouses, health care providers who transmit claims in electronic form, and Medicare prescription drug card sponsors. Individuals such as directors, employees, or officers of the covered entity, may also be directly criminally liable under HIPAA in accordance with principles of “corporate criminal liability.” Where an individual of a covered entity ...Article continued on Page 2

Where can I find the latest forms and other information about HIPAA?

The HIPAA Privacy Compliance Office has developed a website for Purdue staff to access forms and other HIPAA-related information. To access the site, please visit:  http://www.purdue.edu/hipaa or contact: Joan Vaughan, Director, HIPAA Privacy Compliance, x61927
H1N1 Malware Campaign Circulating

On December 2, 2009, The United States Computer Emergency Readiness Team (US-CERT) issued an alert warning of a malware campaign circulating via email messages regarding the H1N1 vaccination. These email messages contain a link to a bogus Centers for Disease Control and Prevention website. Users who click on this link may become infected with malware. Public reports indicate that these email messages are noted as having subject lines such as: “Governmental registration program on the H1N1 vaccination” and “Your personal vaccination profile.” Please note that subject lines may change at any time.

While ITaP Networks and Security (ITNS) reports that this malware campaign is not currently widespread on campus, ITNS recommends that people who receive these emails should delete them immediately without navigating to any websites indicated in the email.

To help mitigate malware risks, ITNS recommends that all users install antivirus software and set it to update daily and to avoid untrustworthy downloads. Additional computer security tips can be found in the security checklist, located at: http://www.purdue.edu/securepurdue/docs/securityChecklist.pdf

To read the US-CERT activity report about the H1N1 malware campaign, visit http://www.us-cert.gov/current/index.html#h1n1_malware_campaign_circulating

HIPAA Penalties for Noncompliance...Continued

is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.

Knowingly

The DOJ interpreted the “knowingly” element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in Violation of the HIPAA statute is not required.

Definitions:

Reasonable cause means circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.

Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

FAQ of the Month

Provided by the Office for Civil Rights

Question:

Is the HIPAA Privacy Rule suspended during a national or public health emergency?

Answer:

No; however, the Secretary of HHS may waive certain provisions of the Rule under the Project Bioshield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act.

What provisions may be waived

If the President declares an emergency or disaster and the Secretary declares a public health emergency, the Secretary may waive sanctions and penalties against a covered hospital that does not comply with certain provisions of the HIPAA Privacy Rule:

- the requirements to obtain a patient’s agreement to speak with family members or friends involved in the patient’s care (45 CFR 164.510(b))
- the requirement to honor a request to opt out of the facility directory (45 CFR 164.510(a))
- the requirement to distribute a notice of privacy practices (45 CFR 164.520)
- the patient’s right to request privacy restrictions (45 CFR 164.522(a))
- the patient’s right to request confidential communications (45 CFR 164.522(b))

When and to what entities does the waiver apply

If the Secretary issues such a waiver, it only applies:

- In the emergency area and for the emergency period identified in the public health emergency declaration.
- To hospitals that have instituted a disaster protocol.

The waiver would apply to all patients at such hospitals. For up to 72 hours from the time the hospital implements its disaster protocol.

When the Presidential or Secretarial declaration terminates, a hospital must then comply with all the requirements of the Privacy Rule for any patient still under its care, even if 72 hours has not elapsed since implementation of its disaster protocol.

Regardless of the activation of an emergency waiver, the HIPAA Privacy Rule permits disclosures for treatment purposes and certain disclosures to disaster relief organizations. For instance, the Privacy Rule allows covered entities to share patient information with the American Red Cross so it can notify family members of the patient’s location. See 45 CFR 164.510(b)(4).