Finally, the Final HIPAA/HITECH Regulations are Here!

By

LYNDA M. JOHNSON

Friday, Eldredge & Clark
Published on January 17, 2013. First published as proposed regulations way back in 2009!!

Effective on March 26, 2013

Compliance Deadline is September 23, 2013
Highlights of the Final Regulations

Implementation of Tiered Penalty Structure for HIPAA Violations
New tiered penalty applies to violations occurring after February 18, 2009.

New maximum penalty for violation of the same HIPAA provision is $1.5 million per year. Prior to HITECH, the maximum was $25,000 per year.
<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>Total CMP for Violations of an Identical Provision in a Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknowing</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>At least $50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Important to note that if a breach involves the PHI of 1,000 individuals, the breach will be considered 1,000 violations of the same provision.

Also, when the violation is continuous over a period of time, for penalty purposes, the number of identical violations will be based on the number of days the inadequate safeguards were in effect. For example, if an inadequate safeguard, such as not following the minimum necessary rules, was in place for 60 days, there are 60 violations of the same provision.
If the event involves two violations – a breach involving 1,000 individuals and an inadequate safeguard for 60 days, a separate penalty may be assessed for each violation. This means the annual penalty cap would be $3 Million - $1.5 Million for each violation.
Tiered Penalty Structure Establishes four levels of culpability:

- **Unknowing.** The covered entity or business associate did not know and reasonably should not have known of the violation.

- **Reasonable Cause.** The covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission was a violation, but the covered entity or business associate did not act with willful neglect.
Tiered Penalty Structure Establishes four levels of culpability:

- **Willful Neglect-Corrected.** The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA. However, the covered entity or business associate corrected the violation within 30 days of discovery.

- **Willful Neglect-Uncorrected.** The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA, and the covered entity or business associate did not correct the violation within 30 days of discovery.
Given these new penalties, a covered entity or business associate that discovers a HIPAA violation that is not due to “willful neglect” should:

1. Correct the violation within 30 days of the discovery.

2. Document the date on which the violation was discovered.

3. Document the date on which corrective action was implemented to establish a basis for asserting the defense that a penalty should not be imposed.
Important Point: the Secretary of HHS may not impose a CMP for a violation that is not due to willful neglect and that is corrected within 30 days of actual or constructive knowledge of the violation.
The new regs make a covered entity liable for violations of its business associates that are its agents, and make a business associate liable for violations by their agents. Prior to HITECH, covered entities were NOT subject to CMPs for violations by a business associate.
Requirements for Business Associates:

- They must comply with the terms of the business associate agreement.
- They must provide PHI to the Secretary of HHS upon demand.
- Provide an electronic copy of PHI to an individual upon their request.
- Make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
- Enter into business associate agreements with subcontractors that create or receive PHI on their behalf.
The definition of a business associate has changed!! Under the final regs, an entity that merely “stores” or maintains PHI is now a business associate. This means that “cloud” vendors are business associates even if they do not access PHI.
Should review and amend Business Associate Agreements in light of the liability imposed on covered entities for the actions of the business associates.

Also Business Associates are required to enter into written agreements with their contractors under the final regs.

Should consider carefully how to handle breach notification in the Business Associate Agreement.

Also, consider how the covered entity will monitor the business associate’s compliance with the business associate agreement.
Changes to Notice of Privacy Practices:

- Must include statement that some uses and disclosures (marketing, sale of PHI, psychotherapy notes, and other uses and disclosures not described in the Notice) will be made only with authorization.

- A statement regarding an individual’s right to notice in the event of a breach.

- Notice of the right to opt out of fundraising communications.
Changes to Notice of Privacy Practices:

- A statement about the right to receive PHI in an electronic format from the covered entity.

- A statement about an individual’s right to restrict disclosures of PHI to health plans if an individual has paid for the services out of pocket in full.

- Note that the previous requirement that a statement be included if the covered entity intends to contact the patient with appointment reminders or information about treatment alternatives is no longer required and can be deleted.
The revised NPP must be available to existing patients upon request and must be posted both to the provider’s website and in a prominent location on the premises. New patients have to be provided with a copy of the revised NPP.
BIG CHANGES TO BREACH NOTIFICATION
The final regs. eliminate the “harm” element and create a presumption of a reportable breach. A four factor test is set forth to determine whether or not PHI has been compromised, requiring breach notification.
These are the four factors:

1. The nature and extent of the PHI involved in the incident. (whether the PHI is sensitive information like SSN or infectious disease test results)
2. The recipient of the PHI. (whether another covered entity received the PHI)
3. Whether the PHI was actually acquired or viewed.
4. The extent to which the risk has been mitigated following the unauthorized disclosure. (whether it was immediately returned and destroyed)
For breaches affecting fewer than 500 individuals, the final regs clarify that Covered Entities must notify HHS within 60 days after the end of the calendar year in which the breaches were “discovered” and not when the breaches “occurred.”
This change means your breach notification policy must be revised!!
Changes to the Marketing Rules

The final regulations require authorization for all treatment and health care operations communications where the covered entity receives remuneration from the third party whose products or services are being marketed.

However, there are still exceptions for face-to-face communications and for reminders concerning refills of drugs or biological that are currently prescribed to the patient. Also allowed are communications about generic equivalents.
Broader Fundraising Communications

The final regs allow the use of demographic information, dates of service, department of service, treating physician, outcome information and health insurance status for fundraising purposes by fundraising entities and their business associates.
The opportunity to “opt out” of future fundraising communications must be “clear and conspicuous”

The method of “opting out” must not impose an undue burden (writing a letter would impose an undue burden)

The covered entity must not make fundraising communications to the individual after the individual has “opted out. The prior regs required only a “reasonable effort.”
Sale of PHI

The final regs generally prohibit the “sale of PHI” by a covered entity or business associate unless an authorization is obtained or an exception applies.
Sale of PHI

The exceptions include:

1. Disclosures for treatment and payment;
2. Disclosures for public health purposes;
3. Disclosures as part of the sale, transfer, merger or acquisition of a covered entity; or
4. Disclosures required by law.

If any of the exceptions apply, there is no cap on the amount of payment the disclosing covered entity may receive.
Research

The final regs allow an authorization for research purposes to include future research studies and allows compound authorizations for multiple research studies.
Deceased Patients

The final regs limit HIPAA protections to 50 years after an individual’s death. Also, the final regs allow covered entities to disclose a deceased person’s PHI to persons who were involved in the patient’s care or payment for the care. Also, covered entities can continue to communicate with family and friends after an individual’s death, unless it is contrary to the patient’s expressed preferences.
The final regs allow a covered entity to disclose a student’s immunization record to a school upon request of a parent or guardian. The request does not have to be in writing, but I suggest we document the request from the parent.
QUESTIONS

Lynda M. Johnson

Friday, Eldredge & Clark, LLP
Ljohnson@fridayfirm.com
501-370-1553