Health Research Institute
Regulatory Spotlight
pwc.com/hri

February 2014

pwc

Bar raised for handling health information under Final HIPAA Rule

The final version of the HIPAA rule, released by HHS in January 2013, reflects two growing realities among the U.S. health system. First, the rule takes a decidedly consumer-centric approach, strengthening existing patient protections for personal information and limiting how providers, insurers and others may use it. And second, the rule reflects a changing health system that is becoming more and more digital.

Both of those acknowledgments are at work in the latest HHS directive. Although the final rule incorporates much from the interim regulations, core elements have changed. Most notably, the rule adopts a broad definition of a "breach." In the past, the bar for a reportable breach focused on whether or not a person was harmed financially or had their reputation compromised due to lax safeguards. The latest update removes the "harm" provision. Now, an "impermissible use or disclosure of protected health information is presumed to be a breach," unless the health organization demonstrates there is little chance the data has been compromised using a highly specific four-point test.

Business associates share in the liability—and potentially much higher fines. Healthcare providers, insurers, their contractors and subcontractors are liable for noncompliance and breaches. Business associates and subcontractors are now bound by law rather than contract to protect health information. Penalties range from $100 to $50,000 per violation, with a cap at $1.5 million per year, per incident. To compare, the per-violation penalties before the HITECH law were only $100, capped at $25,000 per incident, per year.

Patients can restrict access to medical data even between insurers and providers. Under the final rule, individuals can restrict access to their health data even between providers and insurers if they decide to pay out of pocket instead of through their coverage or prescription drugs. Healthcare providers are required to explain the measure in writing to patients. The rule also prohibits most group health plans and Medigap issuers from using or disclosing genetic information for underwriting.

Sales, marketing and fundraising activities are restricted. Health organizations that receive a payment from a third-party vendor whose product is being marketed must disclose the relationship to the patient. Prescription refill reminders and other communications about prescribed medications are exempt from needing an authorization.

Some organizations may be able to delay the new requirements for a year. The rule requires providers, insurers and their business associates to be fully compliant with the changes.

Personal health information stays protected for decades after a person's death. The final rule keeps privacy and security protections on health information until 50 years after a person's death. Only certain designated individuals can authorize release of the information sooner.

At a glance

Released: January 17, 2013

Effective Date: March 26, 2013
Compliance Date: September 23, 2013

- Adds to the privacy and security measures established under HIPAA. Includes rules for the HITECH Act and the Genentic Information Nondiscrimination Act.
- Makes health entities and business associates directly liable for compliance.
- Strengthens consumer privacy and security provisions.
- Prohibits the sale and marketing of sensitive health data without authorization.
- Gives individuals access to an electronic copy of their health records.
- Individuals who pay out of pocket for clinical treatment or drugs instead of through an insurer can prevent the insurer from getting to see that information.
- Unauthorized disclosure and breaches of health data are presumed compromised and require notification unless proven otherwise.
- Stiffens the per-violation penalties.

Contacts

Ben Isgur (Director)
benjamin.isgur@us.pwc.com
(214) 754-5091

Bobby Clark (Pharma/Life Sciences)
robert.j.clark@us.pwc.com
(202) 312-7947

Matthew DoBias (Provider)
matthew.r.dobias@us.pwc.com
(202) 312-7946

Caitlin Sweany (Payer)
caitlin.sweany@us.pwc.com
(202) 346-5241

© 2014 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the United States member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.