Reinhart

HIPAA New Year! Finally, Final HIPAA Rules Issued

In today's Federal Register, the Department of Health and Human Services, Office for Civil Rights (OCR) published the long-awaited regulations (Final Rule) implementing most of the privacy and security provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which amend the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Final Rule, first issued on January 17, 2013, expands certain HIPAA obligations of business associates and their subcontractors, modifies the breach notification standard, expands patient rights to access and to restrict disclosure of their protected health information (PHI), imposes new requirements on the uses and disclosures of PHI, clarifies OCR's enforcement approach, and addresses obligations under the Genetic Information Nondiscrimination Act of 2008. These changes become effective on March 26, 2013 and most provisions must be complied with by September 23, 2013.

Some highlights of the HIPAA changes include:

New Breach Notification Standard. The Final Rule significantly revises the definition of "breach" to make it more likely notification would be required. Under HITECH, covered entities and their business associates must notify individuals if their unsecured PHI is acquired, accessed, used or disclosed in a manner not permitted under HIPAA that "compromises the security or privacy of the [PHI]." Under the Interim Final Breach Notification Rule, if the covered entity could find that there was no significant risk of "financial, reputational, or other harm to the individual" as a result of the impermissible use or disclosure, the use or disclosure was not deemed to be a breach and notification was not required. Under the Final Rule, any impermissible use or disclosure is presumed to be a breach, requiring notification to the individual, unless the covered entity or business associate demonstrates, through a formal risk assessment, that there is a "low probability" that the PHI was compromised.

To assess the probability that the PHI has been compromised, covered entities and business associates must conduct and document a risk assessment that considers, at minimum, the following four factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4)

POSTED:

Jan 24, 2013

RELATED PRACTICES:

Health Care
https://www.reinhartlaw.com/practices/health-care

RELATED PEOPLE:

Heather L. Fields
https://www.reinhartlaw.com/people/heather-fields

the extent to which the risk to the PHI has been mitigated.

Other changes in the Final Rule regarding breach notification include:

- The previous exception to the definition of breach for a limited data set with birthdates and zip codes removed was eliminated. The unauthorized use or disclosure of such limited data sets is now presumed to be a breach unless a formal risk assessment demonstrates that there is a low probability that the PHI was compromised.
- OCR clarified that minimum necessary violations may trigger breach notification requirements and, therefore, require the formal risk assessment outlined above.

Expanded Definition and Liability of Business Associates. The Final Rule expands the definition of "business associate" to include all entities that create, receive, maintain, or transmit PHI on behalf of a covered entity, including business associate subcontractors, such as certain data storage organizations, to whom a business associate delegates a function, activity or service. It also makes business associates directly liable for compliance with all of HIPAA's security provisions and most of its privacy provisions. Business associates and subcontractors are not subject to certain provisions of the privacy rule, such as providing a notice of privacy practices or designating a privacy official, unless they are delegated these responsibilities through a business associate agreement.

Other important changes in the Final Rule related to business associates include:

- Business associates must now obtain satisfactory assurances from subcontractors in the form of a business associate agreement. Covered entities are not obligated to enter into a business associate agreement with a subcontractor; instead, it is the obligation of the business associate that engaged the subcontractor.
- Covered entities and business associates will have 180 days from publication beyond the effective date of the Final Rule—meaning September 23, 2013—to comply with most of the rule's provisions. Compliant business associate agreements made on or before January 25, 2013 will remain in compliance until they are renewed or modified, or until September 22, 2014.

Covered Entity Use and Disclosure of PHI for Marketing, Fundraising. The

Final Rule enhances restrictions on the use and disclosure of PHI for marketing and fundraising as follows:

- Marketing. The Final Rule requires authorization for all treatment and health care operations communications where the covered entity receives financial remuneration for making the communication from a third party whose product is being marketed. There is still an exception for face-to-face marketing communications by a covered entity to an individual, such as a promotional pamphlet or a gift of nominal value provided by the covered entity. However, the Final Rule clarifies that phone communication does not constitute a face-to-face communication and, therefore, is not subject to the exception.

- Fundraising. Under the Final Rule, covered entities must continue to provide individuals the option to "opt-out" from receiving additional fundraising communications, but may not create an undue burden on the individual or require more than a nominal cost. Additionally, opt-out mechanisms must be reasonably accessible to all individuals wishing to opt-out (e.g., toll-free phone number, e-mail address or self-addressed stamped post card located on the fundraising material). Covered entities must also have data management systems and processes in place to timely track and flag those individuals who have opted out of receiving fundraising communications to ensure that they are not sent any additional fundraising communications. Finally, the Final Rule expands the types of PHI that may be used for fundraising to include information regarding a department of service (e.g., cardiology, oncology), a treating physician, health insurance, or outcomes (e.g., death of the patient or any sub-optimal result of treatment or services in order to avoid sending materials to an individual who has recently died or received a terminal diagnosis).

Covered Entities Must Revise Their Notice of Privacy Practices. Changes in the Final Rule will require updates to covered entities' notice of privacy practices (NPP). While covered entities will no longer have to include a statement regarding the use and disclosure of PHI for treatment-related marketing-type communications or appointment reminders, the Final Rule requires covered entities to include various new rights notifications in their NPP, including:

- The prohibition on the sale of PHI;

- The individual's right to opt-out of receiving fundraising communications;

- The individual's right to be notified following a breach of unsecured PHI; and
- The individual's right to restrict disclosure of PHI to a health plan with respect to treatment for which the individual has paid fully out-of-pocket.

Enforcement Clarified. OCR's enforcement authority was significantly strengthened by HITECH, and the Final Rule clarifies that OCR may move directly to a civil money penalty without first attempting to resolve HIPAA violations by informal means. The Final Rule also requires OCR to formally investigate complaints indicating violations due to willful neglect and impose monetary penalties for such violations. The enforcement provisions in the Final Rule become effective on March 26, 2013.