

Major changes affecting health information privacy

By Kimberly Ruppel and Rosanna Willis

Health care reform. Obamacare. The Affordable Care Act. Whichever term you use, privacy and protection of personal health information is one area of concern to insurers, health care providers, employers and individuals alike.

If your practice area touches any of these types of clients, it is important to keep abreast of changes to this area of the law in order to avoid the potential for significant fines or penalties that may be imposed by a breach of the security or privacy rules.

On Jan. 17, 2013, the Department of Health and Human Services issued a final rule modifying the Health Insurance Portability and Accountability Act's Privacy, Security, and Enforcement Rules, which impact the Health Information Technology for Economic and Clinical Health Act as well as the Genetic Information Nondiscrimination Act of 2008.

Generally speaking, the purpose of the Final Rule is to strengthen the privacy and security protections for individual's health information and to reduce the burden imposed on the entities that maintain such information, including health insurers and their "business associates."

More specifically, the Final Rule, which becomes effective March 26, 2013, contains four sub-parts which in turn are designed to:

- Strengthen privacy and security protections;
- Modify the "breach notification" rule;
- Strengthen privacy protections for genetic information; and
- Otherwise modify HIPAA to improve workability and effectiveness and to increase flexibility for and decrease burden on regulated entities.

Covered entities and business associates must comply with the final rule by Sept. 23, 2013.

Business associates

The Final Rule expands the potential for liability resulting from improper disclosure of PHI to a "covered entity" or its "business associate," which is expressly defined as an entity which requires "access to protected health information on a routine basis."

Entities that "act as mere conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis are not business associates." This test can include health information organizations, e-prescribing gateways or their subcontractors.

New standard for breach notification

The Final Rule created a new "Low Probability" standard that covered entities and business associates must use to determine whether an impermissible use

or disclosure of unsecured PHI is a "breach" requiring notification to the Secretary of HHS, affected individuals, and/or to the media.

The new "low probability" standard replaces the previous "harm standard." Under the Final Rule, a covered entity's determination of whether there is a "low probability" that PHI was compromised must address, at the least, the following four factors:

- The nature and extent of the PHI involved;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

The Final Rule includes a presumption that a breach has occurred unless it is demonstrated, through the use of the Low Probability standard, that a breach did not occur.

Notice of Privacy Practices

The Privacy Rule prescribes certain information that must be included in a covered entity's Notice of Privacy Practices, including a statement that any use or disclosure of PHI other than those permitted by the Privacy Rule will be made only with written authorization of the individual, which may be revoked.

Also, if the covered entity records or maintains psychotherapy notes, then its NPP must include a statement that use and disclosure of psychotherapy notes re-

quire an individual's written authorization. If the covered entity is a health plan and it uses or discloses PHI for underwriting purposes, then its NPP must state that the covered entity is prohibited from using or disclosing genetic information for such purposes. All covered entities must include in their NPP a statement of the right of affected individuals to be notified following a breach of unsecured PHI.

Access of individuals to PHI

The Final Rule implements the change made by the HITECH Act, which requires a covered entity to allow an individual to access an electronic health record (EHR) in electronic format. Access must generally be provided within 30 days of the request.

GINA

The Final Rule implements changes made by GINA to explicitly state that health information includes genetic information, and to prohibit all types of health plans covered by the Privacy Rule — other than issuers of long-term care policies — from using or disclosing genetic information for underwriting purposes.

The Final Rule adds applicable definitions from GINA, including genetic information, genetic services and genetic tests. The Final Rule clarifies that information about manifested diseases or disorders of the individual, or conditions or medical tests of the individual, such as an HIV test, complete blood count, or cholesterol or liver function test, are not genetic information and may be used or disclosed for underwriting purposes.

The Final Rule defines "underwriting purposes" to mean:

- Rules for eligibility or benefits;
- Determination of premium or contribution amounts;
- The application of any pre-existing condition exclusion; and
- Other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits.

"Underwriting purposes" does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, if genetic information is relevant to the coverage decision.

Marketing activities

The Privacy Rule requires that covered entities obtain a valid authorization from individuals before using or disclosing PHI to "market" a product or service.

"Marketing" is defined as "communication about a product or service that encourages recipients of the communication to purchase or use the product or service" and generally excludes communications for treatment and health care operations purposes.

The Final Rule's changes to the definition of "marketing" concern its exceptions, which are now dependent upon any "financial remuneration" received.

Kimberly Ruppel and Rosanna Willis are attorneys at Dickinson Wright PLLC. Ruppel focuses her practice on insurance and commercial litigation matters. Contact her at (248) 433-7291 or kruppel@dickinsonwright.com. Willis focuses her practice on assisting healthcare providers and suppliers with corporate transactional and regulatory matters. Contact her at (248) 433-7584 or rwillis@dickinsonwright.com.



©iStockphoto.com