

Authors

Jennifer L. Rangel
512-305-4745
jrangel@lockelord.com

Denise E. Hanna
202-220-6992
dhanna@lockelord.com

Lindsay Setliff
512-305-4808
lsetliff@lockelord.com

Tammy M. Ward
512-305-4776
tward@lockelord.com

www.lockelord.com

This *Client Alert* is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. Readers should obtain legal advice specific to their enterprise and circumstances in connection with each of the topics addressed.

If you would like to be removed from our mailing list, please contact us at either unsubscribe@lockelord.com or Locke Lord Bissell & Liddell LLP, 111 South Wacker Drive, Chicago, Illinois 60606, Attention: Marketing. If we are not so advised, you will continue to receive *Client Alerts*.

Attorney Advertising

© 2010 Locke Lord Bissell & Liddell LLP

HIPAA Security and Privacy Rules Modified for HITECH Act Provisions

On Wednesday, July 14, 2010, the U.S. Department of Health and Human Services (HHS) published proposed modifications (the Proposed Rule) to the HIPAA Privacy & Security Rules. If adopted, the Proposed Rule will guide the implementation and enforcement of HIPAA changes that were passed last year by Congress in the HITECH Act of 2009, and significantly affect how activities of Covered Entities, Business Associates and others are regulated and monitored. The Proposed Rule further elaborates and expands upon some of the measures adopted in the HITECH Act.

Most notably, the new Proposed Rule focuses on the following areas concerning HIPAA:

- Expansion of individuals' rights to access their information;
- Requirements for Business Associates of HIPAA-Covered Entities to be subject to most of the same rules as Covered Entities;
- Mandated changes to Business Associate agreements;
- New limitations on the use and disclosure of protected health information (PHI) for marketing and fundraising; and
- The sale of PHI without patient authorization.

We shall address these and other requirements under the Proposed Rule in more detail below.

Meaning of "Business Associate" Expanded

Pursuant to the HITECH Act, the Proposed Rule expands the pool of "services providers" that qualify as HIPAA Business Associates and defines "Business Associate" to expressly include Patient Safety Organizations, Health Information Exchange Organizations, e-prescribing gateways,

vendors of personal health records and other persons that facilitate data transmission. Moving beyond the statutory language of the HITECH Act, HHS also is proposing that subcontractors working at the direction of or on behalf of a Business Associate and who handle PHI would be required to comply with the applicable Privacy and Security Rule provisions in the same manner as the primary Business Associate, and likewise would incur liability for acts of noncompliance. With the inclusion of subcontractors in the definition of Business Associate, the Proposed Rule requires a Business Associate to obtain satisfactory assurances from the subcontractor to protect the security of electronic PHI it receives and imposes breach notification requirements on subcontractors if a breach of unsecured PHI occurs.

Privacy and Security Rules Expanded for Business Associates

One of the most significant changes resulting from the HITECH Act is the expansion of HIPAA's Privacy and Security Rules to Business Associates. Prior to the HITECH Act, violations of HIPAA were generally not directly enforceable against Business Associates, and a Covered Entity was not generally liable for, or required to monitor, the actions of its Business Associates unless it discovered a material breach or violation of the contract by the Business Associate. The HITECH Act, however, made Business Associates liable for compliance with both the Security Rule and the use and disclosure provisions of the Privacy Rule in the same manner as those requirements apply to Covered Entities. In furtherance of that end, the Proposed Rule

modifies existing regulations to clarify that, where provided, the standards, requirements, and implementation specifications of the HIPAA Privacy, Security and Breach Notification Rules apply to Business Associates. For example, it expressly extends to Business Associate's responsibility for compliance with the HIPAA Security Rule's administrative, physical, and technical safeguard requirements.

Updating Business Associate Agreements

While Business Associates are now directly liable for civil money penalties under the HIPAA Rules for impermissible uses and disclosures of PHI, they also are contractually liable to Covered Entities pursuant to their Business Associate agreements. The Proposed Rule would require the following specific modifications to Business Associate agreements to enhance the contractual rights of Covered Entities and obligations of Business Associates: (1) that Business Associates comply, where applicable, with the Security Rule with regard to electronic PHI; (2) that Business Associates report breaches of unsecured PHI to Covered Entities; and (3) that Business Associates ensure that any subcontractors that create or receive PHI on behalf of the Business Associate agree to the same restrictions and conditions that apply to the Business Associate with respect to such information. The Proposed Rule further clarifies that a Business Associate is contractually liable not only for uses and disclosures of PHI, but also for all other requirements of the Privacy Rule, as they pertain to the performance of the Business Associate's contract with the Covered Entity.

In recognizing the anticipated administrative burden and cost to implement revised Business Associate contract provisions of the Privacy and Security Rules, HHS proposes new transition provisions to allow Covered Entities and Business Associates (and with Business Associate subcontractors) to continue to operate under existing contracts for up to one year beyond the compliance date of final rule.

Changes to an Individual's Right to Access

The Proposed Rule implements HITECH provisions that strengthen an individual's right of access to their electronic health records. The rule requires that if the PHI requested is maintained electronically, the Covered Entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, if not, in a readable electronic form and format as agreed by the Covered Entity and the individual. The Proposed Rule also provides that, at the request of the individual, a Covered Entity must transmit a copy of PHI directly to another person designated by the individual. Such a request, however, must "be in writing, signed by the individual, and clearly identify the recipient of the PHI." For such service, the Covered Entity could only charge the cost of the supplies and labor for copying the PHI, the cost of postage associated with mailing the PHI and, if applicable, the cost of preparing an explanation or summary of the PHI.

Under the current requirements, an individual's request for access must be approved or denied, and if approved, access or a copy of the information

provided within 30 days. Where records requested are only accessible from an off-site location, the Covered Entity has an additional 30 days to respond to the request and, in extenuating circumstances, where access cannot be provided within these timeframes, the Covered Entity may have a one-time 30-day extension if the individual is notified of the need for the extension within the original timeframe. In issuing the Proposed Rule, HHS requested public comment with regard to these timeliness standards and efficiencies for providing responses.

Limitations on Marketing and Sale of PHI

The Privacy Rule requires Covered Entities to obtain valid authorization from individuals before using or disclosing their PHI to market a product or service to them. The HITECH Act adds additional limitations to the authorization requirement. To implement the new marketing limitations of the HITECH Act, the Proposed Rule (1) refines what defines "marketing" communications (for which an individual's authorization is required) to better distinguish them from communications for health care treatment or health care operations (for which authorization is not required); (2) adds a definition of "financial remuneration;" (3) provides that health care operations communications for which financial remuneration is received by the Covered Entity constitute marketing and requires an individual authorization to send such communications; (4) provides that written treatment communications for which financial remuneration is received by the Covered Entity are

subject to certain notice and opt out conditions; and (5) provides a limited exception from the remuneration prohibition for prescription refill reminders. For purposes of this rule, "financial remuneration" means direct or indirect payment from or on behalf of a third party whose product or service is being described, but excludes any direct or indirect payment for the treatment of an individual.

Limitations of Fundraising

The HITECH Act requires HHS to issue a rule relating to a Covered Entity's responsibilities to provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt-out of receiving any further fundraising communications. Additionally, the HITECH Act states that if an individual does opt-out of receiving further fundraising communications, the individual's choice to opt-out must be treated as a revocation of authorization under the Privacy Rule. The proposed new rule not only addresses this requirement but also provides that the method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden of more than nominal cost. HHS encourages Covered Entities to consider the use of a toll-free phone number, an e-mail address, or similar opt-out mechanism that would provide individuals with a simple, quick and inexpensive way to opt-out of receiving future communications. HHS notes that it would place an undue burden on individuals if they were required to send a letter to the Covered Entity asking not to receive future fundraising communications. HHS also provides that it would be unlawful for a Covered

Entity to condition treatment or payment on an individual's choice with respect to receiving fundraising communications. While the HITECH Act imposes an obligation on a Covered Entity to make "reasonable efforts" to ensure that those individuals who have opted-out of receiving fundraising communications are not sent such communications, the proposed new rule goes further and prohibits a Covered Entity from sending fundraising communications to an individual who has elected not to receive such communications.

In the area of fundraising, HHS is soliciting public comment on several topics. These include describing what fundraising communications to which an opt-out should apply, how to opt-back into receiving fundraising materials and limits on information that may be used or disclosed for fundraising demographic information.

Minimum Necessary

The HITECH Act mandated that HHS issue additional guidance on what constitutes "minimum necessary" use of PHI under HIPAA's Privacy Rule. At this time, HHS is proposing to leave the current regulatory text unchanged. HHS is soliciting public comment on what aspects of the minimum necessary standard Covered Entities and Business Associates believe would be most helpful for HHS to address in further guidance and the types of questions entities may have about how to appropriately determine the minimum necessary use standards for purposes of complying with the Privacy Rule.

With that said, the new Proposed Rule expressly expands the "minimum necessary" standard to Business Associates, providing that a Business

Associate's use, disclosure or request of PHI must be limited to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Failure to abide by this standard will subject the Business Associate to direct enforcement under HIPAA.

Revisions to Notices of Privacy Practices

The new Proposed Rule amends regulations relating to content of Notices of Privacy Practices (the Notice). Generally, the Notice describes the uses and disclosures of PHI that a Covered Entity is permitted to make, the Covered Entity's legal duties and privacy practices to protect PHI, and the individual's rights concerning PHI. Among the changes proposed, the Notice would need to describe the uses and disclosures of PHI that require an authorization and specify that other uses and disclosures not contained in the Notice and marketing communications would be made only with the individual's authorization. If this rule is finalized, Covered Entities will be required to update their Notice to incorporate the new requirements.

Enforcement and Penalties

The new Proposed Rule also modifies provisions of the Privacy Rule to reflect the liability imposed on a Business Associate by the HITECH Act. Accordingly, HIPAA enforcement actions can be asserted directly against a Business Associate for unauthorized use or disclosure PHI and for violation of HIPAA's new breach notification requirements.

Offices

Atlanta

Austin

Chicago

Dallas

Houston

London

Los Angeles

New Orleans

New York

Sacramento

San Francisco

Washington, DC

HIPAA Security and Privacy Rules Modified for HITECH Act Provisions (cont'd.)

The Proposed Rule also expands provisions relating to penalties for HIPAA violations by Covered Entities or Business Associates. These penalties were strengthened by the HITECH Act and implementing regulations that were published in an interim final rule on October 30, 2009. In the new Proposed Rule, HHS clarifies several aspects of how the agency will assess HIPAA violations and enforce penalties, including clarification regarding the culpability required for each tier of civil monetary penalty created by the HITECH Act. For example, HHS proposes to amend the definition of "reasonable cause" to clarify the scope of violations that will come within the reasonable cause category of violations, including those circumstances that would make it unreasonable for the Covered Entity or Business Associate, despite the exercise of ordinary business care and prudence, to comply with the provision, as well as those circumstances in which a Covered Entity or Business Associate has knowledge of a violation but lacked the conscious intent or reckless indifference associated with the willful neglect category of violations.

Conclusion

In light of expanded HIPAA obligations, increased penalties and more aggressive enforcement under the HITECH Act and its Proposed Rule, Business Associates and Covered Entities must carefully consider their new HIPAA obligations to ensure that they maintain ongoing compliance. If finalized, a number of the proposed changes would require updated or new Business Associate agreements and Notices of Privacy Practices. In addition, the Proposed Rule would significantly impact practices relating to the exchange of PHI and use of PHI for marketing and fundraising. If you should have any questions concerning the new Proposed Rule or would like assistance in

furnishing comments being solicited by HHS, please contact one of the Locke Lord attorney listed on page one. Requested comments in these areas are due by September 14, 2010.

About the Authors

Jennifer L. Rangel is a partner at Locke Lord. Ms. Rangel focuses her practice on regulatory, transactional, and administrative health law. She represents healthcare and managed care organizations in a variety of matters, including HIPAA, Medicare/Medicaid reimbursement issues and fraud and abuse cases related to the Anti-Kickback Act and Stark issues.

Denise E. Hanna is a partner at Locke Lord. She has been involved in public policy and transactional matters affecting the health care industry for more than 20 years. Ms. Hanna has represented health care payors and providers, pharmacy benefit management (PBM) companies, third party administrators, trade associations and other health care organizations in a range of transactional matters and in legislative, regulatory and administrative proceedings.

Lindsay Setliff is an associate in Locke Lord's Austin office. Ms. Setliff focuses her practice in health care.

Tammy M. Ward is an associate in the Austin office whose principal area of practice focuses on transactional, regulatory and administrative health law issues.