HINSHAW
& CULBERTSON LLP

Health Law ALERT

Fewer Than 90 Days and Counting . . . Are You Ready for the HIPAA Compliance Deadline?

July 3, 2013

Covered entities and business associates have fewer than 90 days, or until September 23, 2013, to come into full compliance with the HIPAA Omnibus Final Rule (the "HIPAA Final Rule"). The HIPAA Final Rule details several new requirements for covered entities and business associates and requires changes in policies and procedures of covered entities and business associates. It expands the definition of "business associate" to vendors and subcontractors who may not even be aware they are covered by HIPAA; makes business associates directly responsible for keeping data safe and secure; and expands criminal and civil penalties for covered entities and business associates who violate HIPAA.

Compliance with these new requirements will require substantial time and effort. Covered entities and business associates only have a short time to bring themselves into compliance with the mandatory changes required by the HIPAA Final Rule. It is essential that policies and procedures, forms and agreements reflect both the HIPAA Final Rule's requirements and the covered entity or business associate's actual practices. Significant fines may be imposed for failure to comply with internal process and practice. Compliance with the HIPAA Final Rule is mandatory. The potential consequences for violations are severe and include civil monetary penalties as well as criminal penalties.

Covered entities and business associates should immediately begin to address the action items below. Note, these are only examples and are not a complete list of changes required by the Final Rule.

For Covered Entities (Providers, Facilities, Health Systems, Clearinghouses and Group Health Plans)

Business Associate Agreements

- Update your business associate agreement templates to comply with the HIPAA Final Rule.
- Identify each business associate you deal with to ensure that you have a current, signed, up-to-date business associate agreement that complies with the HIPAA Final Rule.
- Inventory each of your vendors and subcontractors who have access to, use, disclose or create protected health information (PHI) to determine if they are business associates.
- Ensure that you have current, signed, up-to-date business associate agreements with any vendors or subcontractors who have access to, use, or disclose PHI on your behalf.

- Be aware that the definition of “business associate” has been expanded and that vendors and subcontractors (including accountable care organizations, accountants, attorneys, consultants, technology vendors and other service-related vendors) may not be aware that they are now a business associate and have new legal obligations to protect the privacy and security of PHI and to develop and implement HIPAA training, policies and procedures.

- Develop and implement a strategy for amending/renegotiating existing business associate agreements so that up-to-date signed agreements that comply with the HIPAA Final Rule are in place no later than September 23, 2013.

- Develop policies and procedures to address new subcontractor requirements.

- Develop policies and procedures for monitoring business associate HIPAA compliance.

- Develop policies and procedures to ensure that as you add vendors or subcontractors you determine whether a business associate agreement is necessary.

Patient Rights

- Review and modify HIPAA policies and procedures to address new requirements for protecting psychotherapy notes.

- Review and modify HIPAA policies and procedures concerning marketing, fundraising and restrictions on the sale of PHI.

- Review and modify HIPAA policies and procedures on research, decedents, student immunization records, and use of genetic information in underwriting.

- Review and revise HIPAA policies and procedures concerning notices of breaches, right to restrict disclosures, to access electronic PHI, and to designate third parties who may receive PHI.

- Update forms to reflect changes required by the HIPAA Final Rule.

Notice of Privacy Practices

- Update your notice of privacy practices to comply with the HIPAA Final Rule.

- Establish and implement a mechanism for distributing your revised notice of privacy practices.

Marketing, Fundraising and Sale of PHI

- Determine whether your organization uses PHI to promote a product or service, and if so, whether you need to obtain an authorization.

- Review and modify existing HIPAA policies and procedures and forms to address new marketing requirements.

- Review and modify your fundraising policies and procedures to comply with the HIPAA Final Rule, including developing a database for fundraising that allows recipients to opt out and not receive fundraising communications.

- Review your business operations to determine if you are selling PHI and if so, whether you are using authorizations that comply with the HIPAA Final Rule.

Research

- Review your research activities and your authorizations to ensure that they comply with the HIPAA Final Rule.

Breach Notification

- Develop, implement and document processes for conducting risk assessment to determine the probability of compromise of PHI in the event of a breach of unsecured PHI.

- Develop and implement a breach response/security incident reporting program.

- Develop a notification process in the event of a breach, and integrate state breach notification requirements with HIPAA breach notification requirements.

Workforce Education and Training

- Train workforce members on their new privacy, security, risk assessment and breach notification responsibilities and on the new policies, procedures and forms. Workforce members should be trained to identify and report breaches of unsecured PHI in a timely manner.

- Integrate training and compliance into workforce evaluation and disciplinary procedures.

- Ensure that your workforce is trained on compliance with the new business associate requirements.

- Ensure that training is documented and that you have mechanisms in place for auditing and ensuring workforce compliance.

For Business Associates and Subcontractors

Familiarize yourself with the requirements for business associates under the HIPAA Final Rule, recognizing that business associates who have access to PHI are directly liable for compliance with the HIPAA privacy and security rules and are subject to civil fines and criminal penalties for violations.

Business Associate Agreements

- Update your business associate agreement templates to comply with the HIPAA Final Rule.

- Ensure that you have signed up-to-date business associate agreements with all covered entities.

- Evaluate your relationship with vendors and subcontractors and determine if they are business associates.
- Ensure that you have signed-up-to-date business associate agreements with all subcontractors or vendors who have access to, use, or disclose PHI on your behalf.

Privacy Rule Requirements

- Ensure that you have policies and procedures required by the privacy rule concerning the use, disclosure and protection of PHI as required by the privacy rule for business associates.

Security Rule Requirements

- Designate a security official.
- Perform a risk assessment of your information security processes and procedures and establish reasonable safeguards to ensure that PHI is secure and not subject to intentional or inadvertent breaches.
- Implement appropriate administrative, physical and technical safeguards to address vulnerabilities identified in your risk assessment.
- Develop and implement policies, procedures and forms addressing security obligations for PHI.
- Develop policies and procedures to monitor subcontractor business associate compliance with HIPAA.

Breach Notification

- Develop and implement processes to discover breaches of unsecured PHI.
- Develop and implement a process to conduct and document risk assessments for determining the probability of compromise of PHI in the event of a breach.
- Develop and implement a breach response/security incident reporting program.
- Develop a notification process in the event of a breach, and integrate state breach notification requirements with HIPAA breach notification requirements.

Workforce Education and Training

- Train relevant workforce members on their revised privacy, security and breach notification policies. Workforce members should be trained to timely identify and report breaches of unsecured PHI.
- Ensure that training is documented and that you have mechanisms in place for auditing and ensuring workforce compliance.

How We Can Help

Hinshaw & Culbertson LLP attorneys have extensive experience developing and advising on privacy and information security programs. If you have questions or need assistance in determining how to make the requisite changes to your policies, procedures, and practices in order to come into compliance with the Final Rule, please call Michael A. Dowell, Carol D. Scott or your regular Hinshaw attorney.

Hinshaw & Culbertson LLP prepares this publication to provide information on recent legal developments of interest to our readers. This publication is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. We would be pleased to provide such legal assistance as you require on these and other subjects if you contact an editor of this publication or the firm.

Copyright © 2013 Hinshaw & Culbertson LLP. All Rights Reserved. No articles may be reprinted without the written permission of Hinshaw & Culbertson LLP, except that permission is hereby granted to subscriber law firms or companies to photocopy solely for internal use by their attorneys and staff.

ATTORNEY ADVERTISING pursuant to New York RPC 7.1. The choice of a lawyer is an important decision and should not be based solely upon advertisements.