haynesboone
Setting precedent.

Healthcare Alert

January 25, 2013

HHS Provides Amendments to HIPAA Privacy and Security Regulations to Conform Regulations to HITECH, GINA and Add Some Additional Changes

The long awaited Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulation amendments (the "Changes") to incorporate the changes made by Health Information Technology for Economic and Clinical Health (HITECH) in 2009 as part of the American Recovery and Reinvestment Act and by the Genetic Information Nondiscrimination Act ("GINA") were recently released. The Final Rule can be found here.

The Changes affect business associates and covered entities including health plans, healthcare providers and healthcare clearinghouses.

Application of the Changes to Employer Sponsored Group Health Plans and Other Health Plans

What new deadlines must my group health plan meet?

Changes to Policies, Procedures, Training and Operation of the Group Health Plan

The Changes become effective on September 23, 2013 as a general rule. This is the date by which privacy policies, notices, and training will need to be updated. There are special transition rule deadlines for business associate agreement updates. Each group health plan's policies, procedures, privacy notice and training should be reviewed to verify compliance. Note that there is no extended deadline for small plans: all plans are treated equally in the compliance deadlines and in the transition rules.

New Privacy Notices

The Changes impose a number of additional requirements that must be incorporated into the notice of privacy practices each group health plan must provide to participants. *The notice of privacy practices must be updated for the Changes and this requirement does not have a delayed effective date or any special transition rule beyond September 23, 2013.* So as employers are preparing for open enrollment for calendar year plans facing the 2014 health reform changes, they must also be working to meet the deadline for issuing the new updated HIPAA Privacy notice by September 23, 2013.

HIPAA Privacy notices must generally be provided at least every three years and to each new enrollee and at any time there is a material change in the contents of the notice. So once a group health plan's notice is updated, it needs to be sent to the participants. There are also electronic posting rules that have been modified by the Changes.

Business Associate Agreements Changes

The Changes impact the requirements that business associate agreements must meet for a group health plan to be compliant with HIPAA Privacy and Security. The Changes provide a transition period for some business associate agreements.

Entities with a business associate agreement that is currently under negotiation, will only be able to take advantage of the transition period to delay compliance if it is signed by January 25, 2013.

Business associate agreements entered into after January 25, 2013 do not qualify for the transition rule and will need to comply with the Changes when executed.

For business associate agreements entered into prior to January 25, 2013 (i.e., those business associate agreements for a group health plan's service providers that currently are in existence), if those agreements comply with the law that was applicable as of January 25, 2013, and if they are not renewed or modified between March 26, 2013 and September 23, 2013, then they are deemed to be compliant with the Changes until the earlier of (1) the date each contract is renewed or modified on or after September 23, 2013, or (2) September 22, 2014.

For a group health plan that has a business associate agreement that is in effect and compliant on January 25, 2013 that does not renew between March 26, 2013 and September 23, 2013, then no update is required until it is renewed or modified, or, if earlier, September 22, 2014. However, the preamble to the regulation indicates that contracts that automatically renew pursuant to an evergreen clause are still eligible for the extended due date for becoming compliant and do not need to be updated as of the automatic renewal prior to September 23, 2013.

The Changes do not address how a business associate agreement in effect and compliant on January 25, 2013, and that is renewed or modified between January 25, 2013 and March 26, 2013 is to be treated, and whether it might qualify for the deemed compliance transition period or if it must be compliant when signed.

If an entity has a business associate agreement that would otherwise qualify for the transition rule, but it is renewed on or after March 26, 2013, it must be updated when it is renewed and the regulation makes no exception for agreements with automatic renewals; however the preamble to the regulation indicates that business associate agreements that automatically renew under an evergreen provision are to be treated as eligible for the transition period and extended due date for amending the business associate agreement.

The renewal date of each business associate agreement must be verified and the status of each agreement's compliance with the Changes must be determined because some plans have already updated to comply with the statutory changes and may have more limited changes necessary to become fully compliant. Each agreement's renewal clause must be analyzed to determine if it is an evergreen renewal and eligible for the extension on the update deadline. Each agreement's contents must be compared to the Changes' requirements to determine whether it qualifies for the transition rule and the extent to which it must be modified and which deadline for modification applies.

The good news. The Department of Health and Human Services (HHS) has provided sample business associate agreement provisions on its website - see here. These updates only address the Changes and do not cover all aspects that one must include to have a complete enforceable business associate agreement. Updating the business associate agreement is only one aspect of getting a covered entity compliant; there are still notice requirements and changes to policies and procedures, and possibly training.

Other Changes for Group Health Plans

The marketing rules were changed to incorporate the protections for genetic information mandated by the Genetic Information Nondiscrimination Act. The Changes also make it clear that case management and care coordination are not marketing activities unless the group health plan receives compensation for those communications.

The Changes require business associates to disclose protected health information to the Secretary of the Department of Health and Human Services to prove their compliance with the provision of the information to individuals using their right to access their protected health information. This is part of the HITECH changes under American Recovery and Reinvestment Act of 2009 (ARRA) to require business associates to be liable for their noncompliance and require changes to the business associate agreements.

The Changes clarify that a covered entity or business associate is not selling protected health information when it transfers information during due diligence in relation to a merger of the covered entities. This works well when two healthcare providers are merging, but it still does not address the common corporate transaction issue of what can be shared when two corporations that are not healthcare providers are engaged in a transaction and the group health plans they each sponsor are not merging at the time of the transaction.

The Changes clarify that protected health information must only be treated as protected health information for 50 years after the individual died.

The Changes also require that additional notice provisions be added if a group health plan uses any protected health information for underwriting, i.e., for seeking to obtain new quotes for insured plans or for stop loss coverage for self-insured plans.

The Changes also address the requirements from HITECH regarding breaches of unsecured protected health information and the notices that must follow such breaches, as well as the related penalties. An entity's notice of privacy practices and policies must also include information related to breach notification requirements now, in addition to other changes.

The Changes also clarify the penalty structure following the amendments by HITECH, including that business associates can be liable for their violations of HIPAA Privacy standards and it is not merely a violation of the business associate agreement any longer.

The Changes expanded the definition of "state" to include not only the 50 states in the union, but also American Samoa and the Commonwealth of the Northern Mariana Islands, in addition to the District of Columbia, the Commonwealth of Puerto Rico, Guam and the Virgin Islands. The state definition is important because HIPAA Privacy preempts State laws that are not contrary to a HIPAA standard except if the state law is necessary to prevent fraud and abuse or to ensure state regulation of insurance and for certain other limited reasons. The addition of the additional jurisdictions as states requires their laws to also be compared to HIPAA Privacy to determine if HIPAA Privacy preempts those laws.

What is the impact of the changes on healthcare providers and business associates?

Providers and their business associates have been awaiting these final regulations which give more detail to the expansion of HIPAA obligations – particularly to business associates. Prior to the HITECH expansion, many business associates would simply say "not my problem" when confronted by providers with HIPAA compliance matters. Other business associates would undertake activities to satisfy the provider but had very little infrastructure around those activities. These Changes provide business associates with the understanding that they are expected to have substantive HIPAA compliance programs including the execution of business associate agreements with subcontractors.

Business Associates

Business associates have become a larger and more integrated part of the quality care delivery system, giving them access and control to greater amounts of Protected Health Information. Under the new rules, they will now have to give serious attention to the required risk analysis and the determination of whether the recommended safeguards are necessary. The extent to which this risk analysis was performed will become vital if Health and Human Services' preliminary review of a complaint suggests that a violation occurred due to "willful neglect." Such a finding now requires that the Secretary conduct a compliance review of the business associate or covered entity involved to determine whether it is compliant with the applicable standards. A HIPAA compliance program that has been analyzed and properly implemented will be a significant factor in the assessment of whether willful neglect exists.

Business associates must also obtain "satisfactory assurances" in accordance with the rules regarding business associate agreements that the subcontractor will appropriately safeguard the information prior to allowing its subcontractor to create, receive, maintain, or transmit Protected Health Information.

Business Associate Agreements

Covered entities and business associates must comply with the Changes by September 23, 2013. So, any business associate agreements entered into after that date must be compliant with the Changes. If the business associate agreements that an entity has in place currently are compliant with 164.314(a) and 164.504(e), it could have until September 22, 2014 to make any necessary revisions if no renewal or modification is necessary.

Initial Contract Effective Date	Deemed compliant if	Qualification for Deemed Status	Deemed compliance expires
Prior to January 25, 2013	Contract complies with 164.314(a) and 164.504(e) that were in effect on date of execution	No contract renewal or modification between March 26, 2013 and September 23, 2013	The earlier of (1) the date of contract renewal or modification on or after September 23, 2013 OR (2) September 22, 2014
Post January 25, 2013	Contract complies with modified rules by September 23, 2013		

The transition rules also gave special consideration to limited data set use agreements, allowing limited data sets to continue to be shared under those agreements as long as they are compliant with 164.514(e) until September 22, 2014, if they are not modified after September 23, 2013.

Business associates that do not have business associate agreements or data use agreements in place with their subcontractors should begin this contracting process immediately.

Marketing

As patient compliance monitoring is outsourced to business associates and business associates engage contractors to assist in the process, the extent to which information can be shared without the patients' specific authorization has been an issue. The new definition of marketing makes it clear that the extent to which a profit is made on the service determines whether it is marketing for purposes of the rule. It continues to be the case that the sharing of Protected Health Information for marketing purposes requires specific authorization. The various entities that have begun to provide patient monitoring and analysis services for profit will have to give significant thought to the manner in which they obtain authorization for their activities.

We expect that business associates will be very busy in their efforts to comply with the Changes while providers will take this opportunity to reevaluate their programs and ensure that their practice and contracts are in compliance with the Changes.

Fundraising

The fundraising rule was revised to allow Covered Entities to share institutionally or with a related foundation not only demographic information generally, but specifically individual information including name, address, other contact information, age, gender and date of birth, without an authorization. The Changes also allow for the use of the department in which the service was given, treating physician, outcome information and health insurance status without an authorization. This information can only be shared, however, if the sharing of the individual information is included in the Notice of Privacy Practices and the individual is given the opportunity to opt out.

For more information on HIPAA, please contact one of the following Haynes and Boone attorneys.

Bill Morrison
214.651.5018
bill.morrison@haynesboone.com

Kenya S. Woodruff
214.651.5446
kenya.woodruff@haynesboone.com