HHS Issues New HITECH/HIPAA Rule: Top Ten Changes

In the most significant re-write of HIPAA since the law was enacted, the Department of Health and Human Services (HHS) issued omnibus HIPAA regulations which will require substantial operational changes for HIPAA covered entities and their business associates. Here are ten important changes:

• Changes to the data breach rule will make more incidents reportable.
• Business associates are directly liable for HIPAA violations and business associate agreements must be modified.
• HIPAA enforcement is moving toward a penalty-based system and away from voluntary compliance.
• Patients have enhanced rights to electronic copies of records and some patient requests for restrictions must be honored.
• HIPAA notices of privacy practices need to be revised.
• The marketing rules require individual authorization for subsidized treatment communications.
• Researchers can obtain permission to use data for future unspecified research.
• Fundraising provisions expand the permissible use of patient data to target appeals.
• Privacy Rule protections expire for persons deceased for more than 50 years.
• Compliance with most of the new requirements will be required on September 23, 2013.

Changes to the data breach rule will make more incidents reportable

HHS made substantial changes to the data breach notification requirements that will make it more difficult to justify a decision not to notify when a security incident occurs. Under the current requirements a breach must be reported only if it poses a “significant risk of financial, reputational, or other harm to the individual.” The new rule eliminates the risk of harm threshold and provides instead that the unauthorized acquisition, access, use, or disclosure of protected health information is presumed to be a data breach unless a covered entity or business associate demonstrates that there is a low probability that the protected health information (PHI) was compromised. In the event of a potential data breach, covered entities and business associates must determine whether there is a low...
probability that PHI has been compromised by performing a risk assessment that addresses at least the following factors:

- the nature and extent of the PHI involved, including the types of identifiers involved and the likelihood of re-identification;
- the unauthorized person who used the PHI or to whom the information was disclosed;
- whether the PHI was actually acquired or viewed; and
- the extent to which risk to the PHI has been mitigated.

If a use or disclosure is not permitted by the Privacy Rule (and does not fall within three narrow exceptions), a breach that must be reported to affected individuals, HHS, and in some cases the media will be presumed. To rebut that presumption, a risk assessment must demonstrate that there is a low probability the data has been compromised. A higher probability of compromise will mean notification is required, regardless of the likelihood of harm to the affected individuals.

Business associates are required to comply with the HIPAA Security Rule, including the provisions related to physical, administrative, and technical safeguards and related documentation requirements. They will need to perform a HIPAA security risk analysis and to put in place HIPAA security policies; the more general security safeguards historically required through business associate contracts are no longer sufficient. Business associates will be directly liable for violations including impermissible uses and disclosures of PHI and the failure to report a breach to their covered entity customers.

Subcontractors who create, receive, or transmit PHI on behalf of business associates will now be considered business associates themselves, and will be subject to direct liability under the HIPAA Rules. For the first time, business associates will be required to obtain full-blown written business associate agreements (BAAs) from their subcontractors and to take reasonable steps to cure the breach or terminate the contract (if feasible) in the event of a material breach by the subcontractor.

Business associate agreements will need to be modified to meet additional requirements. These BAAs now must require that business associates report breaches of unsecured PHI to covered entities. In addition, to the extent a covered entity delegates its obligations under the Privacy Rule, the BAA must require that business associates comply with all Privacy Rule requirements that apply to the covered entity with respect to the performance of those obligations. Acknowledging the costs and burdens associated with revising the agreements, HHS provides an additional one year transition period (until September 22, 2014) for amending existing BAAs that meet certain requirements, unless the parties otherwise amend or renew the existing contract during the period from March 26, 2013 to September 23, 2013 in which the case the BAA must be compliant with the final rule upon the September 23, 2013 compliance date.
HIPAA enforcement moves toward a penalty-based system and away from voluntary compliance

HHS is required by the HITECH statute to move toward a penalty-based system and away from the voluntary compliance framework used in the past. The final rule provides that:

- Civil and criminal penalties can now be applied directly to business associates.
- HHS must investigate any complaint and conduct compliance reviews in all cases where a preliminary review of the facts indicates a possible violation due to willful neglect.
- HHS must impose a civil money penalty for violations due to willful neglect.
- HHS is not required to attempt to resolve cases of noncompliance due to willful neglect by informal means.
- The tiered penalty structure based on different levels of culpability has been finalized. Penalties now range from US$100 to US$50,000 per violation depending on the level of knowledge/willfulness with a US$1.5 million cap per calendar year for multiple violations of identical provisions.
- Covered entities and business associates can be subject to liability for a violation by their business associate agents and subcontractor business associate agents respectively. Detailed guidance for determining when an entity is an agent is provided.
- HHS may disclose PHI obtained in connection with a compliance review or investigation if permitted under the Privacy Act, thereby giving it the ability to share information with other law enforcement agencies (e.g., state attorneys general or the Federal Trade Commission).

Patients have enhanced rights to electronic copies of records

The new regulations establish the right of patient to obtain a copy of their health records in electronic form when such information is maintained by a covered entity (or business associate) in electronic form in a designated record set (regardless of whether it is part of an electronic health record). Covered entities must provide the electronic copy in a machine readable format mutually agreed upon (e.g., MS Word or Excel, text, HTML, text-based PDF), but need not provide individuals with unlimited choice. Notably, HHS clarifies that if requested by the individual, covered entities may provide the electronic copy of PHI through unencrypted e-mail, provided that the covered entity advises the individual of the risk of doing so. In such a case, the covered entity would not be responsible for any unauthorized access of PHI while in transmission or for safeguarding PHI once delivered to the individual.

In addition, the final rule provides individuals with the right to direct covered entities and business associates to transmit an electronic copy of the record directly to a person or entity designated by the individual, regardless of whether the PHI is in electronic or paper form. Such requests must be in writing, signed by the requesting individual and clearly identify to whom and where the information is to be sent. The covered entity may charge a reasonable cost-based fee, but the fee must not be greater than the covered entity's labor and supply costs and may not include a “retrieval fee.” The rule also tightens the time frame for providing access to records by eliminating the existing provision that allowed 60 days to provide access when records are maintained by the covered entity off-site. Under the new rule, covered entities must provide access to all paper and electronic PHI within 30 days of the individual’s request with the option of a one-time 30-day extension available.

Health care providers must honor certain requests to restrict disclosures to health plans

The Privacy Rule provides individuals with a right to request restrictions on the use or disclosure of their PHI, but in most cases a covered entity is not legally required to agree to the request. The new regulations enhance individual rights by requiring health care providers to honor requests to restrict disclosures to health plans for purposes of carrying out payment or healthcare operations if the disclosure is not otherwise required by law and the PHI relates solely to a healthcare item or service for which the individual has paid the covered entity out of pocket and in full. HHS provides operational guidance for implementing this new requirement, including how to handle payment for bundled services, dishonored payments, and requests for follow-up care that is not paid for out-of-pocket. There is no obligation for health care providers to notify downstream providers of an individual’s request for restriction (e.g., notifying a pharmacist or a physician to whom a patient is referred). That responsibility lies solely with the individual.

HIPAA notices of privacy practices need to be revised
The final rule requires several changes to the HIPAA notice of privacy practices. The notice must include a statement regarding the right of affected individuals to be notified following a data breach and describe certain uses and disclosures of PHI that require patient authorization related to psychotherapy notes, marketing, and the sale of PHI. In addition, the privacy notice must inform individuals that the covered entities may not refuse a request to restrict the disclosure of health information to health plans where the individual pays in full out of pocket for the services to which that information relates.

These modifications to a privacy notice are considered by HHS to be material changes that will require covered entities to provide new notices to individuals. Although the Privacy Rule generally provides health plans with only 60 days following a material revision to mail revised hard copy notices to members, HHS is providing a reprieve by permitting health plans that post their notice on their website to prominently post any material change or the revised notice on that website by the rule’s compliance date (September 23, 2013) and provide the new notice or information about the material changes and how to obtain the revised notice, in its next annual mailing. Health plans that do not currently have a customer service website must provide the revised notice, or information about the material change and how to obtain the revised notice, to members within 60 days of the rule’s compliance date. Current requirements for health care providers regarding distribution of a revised notice remain the same.

The marketing rules require individual authorization for subsidized treatment communications

HHS significantly revised the marketing rules by requiring individual authorizations for treatment and health care operations communications for which financial remuneration (i.e., direct or indirect payment) is received from a third party whose services are being promoted. This is a significant departure from the approach taken in the proposed rule, which would have allowed certain subsidized treatment communications provided that individuals were given notice and the opportunity to opt-out. Individual authorization is not required for refill reminders and other communications that describe only a drug or biologic that is currently being prescribed for the individual, provided that the payment is reasonably related to the covered entity’s cost of making the communication; HHS clarifies that this exception applies to adherence communications and communications about generic equivalents.

Researchers can obtain permission to use data for future unspecified research

HHS modified its previously-held interpretation that an authorization for the use or disclosure of PHI for research must be study specific. Under the new rule, an authorization may permit future research provided that the future research is adequately described such that the individual has a reasonable expectation that his/her PHI could be used or disclosed for such future research. In addition, covered entities will be permitted to combine conditioned and unconditioned authorizations for research (e.g., authorization for research activities where treatment is conditioned on signing the authorization and activities where treatment is not conditioned on signing the authorization), provided that the authorization (i) clearly differentiates between the conditioned and unconditioned research components, and (ii) provides the individual with the opportunity to “opt-in” to the unconditioned research activities. HHS gives covered entities, research institutions, and institutional review boards discretion in determining how to differentiate the conditioned and unconditioned research activities and does not prescribe a particular format.

Fundraising provisions expand the permissible use of patient data to target appeals

The final rule expands the type of information covered entities may use to target fundraising appeals to include the department of service, the treating physician and outcome information. This is a significant expansion of the current HIPAA rules which permit the use only of demographic information and dates of health care provided to the patient. Fundraising communications must provide recipients with a clear and conspicuous opportunity to opt-out and the method provided for the opt-out may not cause undue burden or more than nominal costs. Providing a toll-free number or a prepaid postcard are acceptable opt-out methods while requiring the recipient to write and mail a letter is considered too burdensome.

Privacy Rule protections expire for persons deceased for more than 50 years

The Privacy Rule will no longer provide privacy protections for a decedent’s health information to the same extent and in the same manner as living individuals. Under the final rule, the health information of individuals who have been deceased for more than 50 years will no longer be protected by the Privacy Rule at all. In addition, covered entities will be permitted to disclose PHI to a family member or other individual involved in
the care of a decedent, unless this disclosure is inconsistent with a prior expressed preference of the
decedent.

Compliance with most of the new requirements will be required on September 23, 2013.

Hogan Lovells lawyers are assisting our clients implement the privacy and security requirements of
HITECH. We have extensive experience advising on HIPAA, consumer protection, and international
data privacy and security requirements and compliance programs. If you would like additional
information on the HITECH requirements, need assistance developing, or implementing privacy or
data protection programs, or require support in preparing for or managing a data breach, please
contact the Hogan Lovells lawyer with whom you work, or any of the contacts listed.