September 2010

Important Changes to HIPAA Proposed by HHS

A Summary of Proposed Changes to HIPAA Privacy, Security and Enforcement Rules

by Elizabeth Johnson

The following summarizes the major changes to and new provisions of the HIPAA Privacy, Security, and Enforcement Rules proposed by the Department of Health and Human Services (HHS) in its notice of proposed rulemaking published July 14, 2010 (75 Fed. Reg. 40867). Many of these changes are proposed to implement the HITECH Act, but several of the changes go beyond the provisions of the statute. Other topics covered in this rulemaking were not raised by the HITECH Act and are instead proposed to address issues HHS has identified based on its experience interpreting and administering the rules. Some subjects covered by the HITECH Act, such as breach notification and accounting for disclosures from electronic health records, were not covered in this rulemaking and so are not discussed below. The public comment period on this proposed rulemaking ends September 13, 2010. **Unless otherwise noted below, the compliance deadline for these proposed requirements will be 180 days from the date of publication of the final rule.**

While there are many reasons for the regulated community to be concerned about these and other recent changes to HIPAA regulations, some of the more compelling reasons include:

- Covered entities must notify affected individuals, such as patients and customers, in the event of a security breach affecting unsecured protected health information; notification also must be made to the primary regulator (HHS), which has authority to enforce against any legal violation that may have occurred.
- Recent revisions to the Enforcement Rule changed the maximum annual penalty per identical violation from $25,000 to $1.5 million, a 60-fold increase.
- The interim final Breach Notice Rule has been effective for almost one year, during which time more than 140 covered entities have reported to HHS breaches of unsecured PHI affecting more than 4.8 million individuals (and those figures account only for individual breaches that affected more than 500 people each, meaning their occurrence is immediately noted on HHS's website).
- In addition to making HHS compliance audits mandatory, the HITECH Act authorized state attorneys general to enforce HIPAA; the first such action settled with an agreement by the covered entity to implement a corrective action plan and pay $250,000 in damages.
- Two recent enforcement actions by HHS involving the insecure disposal of health information netted a combined $3.25 million payday for HHS; the agency has reportedly said it will apply those moneys to fund additional enforcement actions and audits.
- Business associates now must comply fully with the Security Rule, which imposes substantial administrative, physical, technical, and organizational security requirements.
- If the proposed changes are finalized as written, business associates will be directly liable for HIPAA violations.
- If the proposed changes are finalized as written, covered entities will no longer be able to escape liability for business associates simply by virtue of having put appropriate contracts in place and not having known of any pattern or practice of violations by the business associate.

The attorneys of Poyner Spruill's Privacy and Information Security practice regularly assist clients with HIPAA implementation, and counsel organizations of all shapes and sizes on their HIPAA obligations, compliance posture, and risk. We provide this summary to assist your organization in commenting on these rules or implementing anticipated changes.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

RALEIGH CHARLOTTE ROCKY MOUNT SOUTHERN PINES WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

New Privacy Rights of Individuals

Access to Electronic Protected Health Information

The current Privacy Rule generally provides individuals with the right to access and request copies of their protected health information (PHI). The proposed rules specify that, where the individual requests an electronic copy of PHI, the covered entity must comply with that request if the electronic PHI (ePHI) is maintained in one or more designated record sets and is readily producible in the requested format. If the ePHI is not readily producible in the requested format, covered entities must provide the ePHI in a readable electronic form and format to be agreed upon with the individual. The covered entity may charge a reasonable fee for both the supplies and labor used to provide the ePHI, which fee may not be greater than the actual costs. The fee may reflect only labor costs (and not cost of supplies) if the individual either provides his own electronic media to store the ePHI or requests transmission of the ePHI by email.

If the individual requests that a copy of PHI (whether hard copy or electronic) be provided directly to another person, the covered entity must comply with that request if it is made in writing, signed by the individual, and clearly identifies the recipient and where to send the copy of PHI.

Requests to Restrict Disclosures of PHI Related to Services Paid Out of Pocket

One of the more controversial privacy provisions in the HITECH Act was the requirement that covered entities restrict disclosures of PHI upon an individual's request, provided that:

1. The disclosure is to a health plan for purposes of carrying out payment or health care operations;
2. The disclosure is not otherwise required by law; and
3. The PHI pertains solely to a health care item or service for which the individual has paid the provider in full out of pocket.

A covered entity would not have to honor the individual's request for a restriction if:

1. The disclosure was for treatment purposes;
2. The individual did not pay in full;
3. Some or all of the payment is not made out of pocket; or
4. The disclosure was not to a health plan.

While the proposed rules implement this HITECH Act requirement, HHS foresees some complications in implementation, stating "[d]ue to the myriad of treatment interactions between covered entities and individuals, we recognize that this provision may be more difficult to implement in some circumstances than in others, and we request comment on the types of interactions between individuals and covered entities that would make requesting or implementing a restriction more difficult." HHS has requested comment on factors not elaborated upon by the statute, such as the provider's obligation, if any, to notify downstream providers (such as specialists that may provide treatment of the same condition) of the individual's request, particularly in cases where a prescribing provider may use an electronic system to submit prescriptions to a pharmacy, which in turn may fill the prescription and notify the individual's health plan before the individual actually arrives at the pharmacy and has an opportunity to request restriction of the disclosure. HHS requests comment on whether a requested restriction should be carried forward to downstream providers and what technological capabilities exist that could facilitate efforts to honor individuals' requests for restrictions.

Under the proposed rules, the individual's right to request restrictions on disclosures of PHI in the above-described circumstances must be noted in the covered entity's notice of privacy practices.

Poyner Spruill LLP
ATTORNEYS AT LAW

New and Revised Restrictions on Uses and Disclosures of PHI

The Minimum Necessary Principle

The HITECH Act currently provides that a covered entity will be deemed to have complied with the minimum necessary principle if it limits uses and disclosures of PHI to a limited data set (to the extent practicable). This statutory requirement is currently effective but will sunset on the effective date of guidance HHS is required to issue on compliance with the minimum necessary principle (the statutory deadline to issue that guidance has already passed). In preparation for its release of that guidance, HHS has requested, through this rulemaking, comments on what aspects of the minimum necessary standard covered entities and business associates believe would be most helpful to have HHS address in guidance, and the types of questions these organizations may have about how to appropriately determine "minimum necessary" for purposes of complying with the Privacy Rule. No changes to the principle as currently stated in the Privacy Rule are proposed or anticipated in the future.

(As described below in the discussion of changes affecting business associates, the proposed rules would apply the minimum necessary principle directly to business associates.)

Use of PHI for Marketing

The new rules revise the definition of marketing to refine the types of communications excluded from the term. This adjustment is important because, generally speaking, covered entities are required to obtain a written authorization from individuals in order to use their PHI for marketing. While "marketing" is generally defined as "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service," the following types of communications are specifically excluded:

1. Communications for treatment of an individual by a health care provider, including case management or care coordination for the individual, or communications to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. (If the communication is made in writing and the health care provider receives remuneration in exchange for making the communication, other new restrictions will apply – see category below entitled "Use of PHI for Treatment Communications.")

2. Communications to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

3. Communications for the following health care operation activities, except where the covered entity receives financial remuneration in exchange for making the communication: (a) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including: (i) communications about participating providers in a health care provider network or health plan network, (ii) replacement of, or enhancements to, a health plan, and (iii) health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or (b) case management or care coordination, contacting individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

If the marketing involves direct or indirect financial remuneration, the authorization obtained from the individual must disclose that such remuneration is involved. "Financial remuneration" means "direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual."

Use of PHI for Treatment Communications

Use of PHI for treatment communications made by health care providers in exchange for financial remuneration will not qualify as "marketing" under the proposed rules and so would not necessitate a written authorization from individuals, provided the following two conditions are met:

1. The notice of privacy practices must disclose that such communications may be sent, that the health care provider will receive financial remuneration in exchange for such communications, and that the individual may opt out of receiving such communications at any time.

2. The treatment communication must disclose that the health care provider is receiving financial remuneration in exchange for providing the communication and must provide the individual with a "clear and conspicuous" opportunity to opt out of further treatment communications. The opt-out method cannot be unduly burdensome or cause the individual to incur more than a nominal cost.

HHS is encouraging use of toll-free phone numbers, email addresses, or other easy and cost-free methods for individuals to opt out of receiving these types of treatment communications. HHS has noted that requiring individuals to respond by postal mail could constitute an "undue burden."

Sale of PHI

Like marketing activities, under the proposed rules the sale of PHI for any direct or indirect remuneration (financial or otherwise) generally would necessitate a prior written authorization from individuals, which authorization must recite that the covered entity will receive remuneration for the disclosure. Under the proposed rules, the following exceptions would apply such that PHI could be exchanged for direct or indirect remuneration in the following circumstances without a prior written authorization:

1. Disclosures of PHI for public health activities;
2. Disclosures of PHI for research purposes if the remuneration received is a reasonable cost-based fee to cover the actual cost of providing the PHI;
3. Disclosures of PHI for treatment or payment purposes;
4. Disclosures of PHI for the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence (described in the definition of health care operations);
5. Disclosures of PHI to the individual or to provide an accounting of disclosures to the individual;
6. Disclosures required by law;
7. Disclosures otherwise permitted by the Privacy Rule when performed in accordance with the relevant requirements and the remuneration received is a reasonable cost-based fee to cover the actual cost of providing the PHI, or the fee is otherwise expressly permitted by law (such as state laws that may specify a maximum charge that can be imposed for providing copies of medical records); and
8. Disclosures of PHI for payment purposes (disclosures made to obtain payment will not constitute "sales" of PHI).

Use of PHI for Fundraising

Covered entities are currently permitted to disclose PHI to business associates or institutionally-related foundations for fundraising purposes without individual authorization if the information disclosed is limited to demographic information and the dates on which health care was provided to the individual. The proposed rules require that the covered entity's notice of privacy practices disclose that the individual may be contacted for fundraising purposes and that the individual may opt out of being contacted at any time. In addition, every fundraising communication must include a "clear and conspicuous" option to opt out of further fundraising communications. The opt-out method cannot be unduly burdensome or cause the individual to incur more than a nominal cost. As noted above, HHS encourages use of toll-free phone numbers, email addresses, or other easy and cost-free methods for individuals to opt out of receiving fundraising communications and has noted that requiring individuals to opt out via postal mail could constitute an "undue burden." Importantly, treatment and payment may not be conditioned on the individual's choice with respect to receipt of fundraising communications.

Compound Research Authorizations

Generally speaking, authorizations required by the Privacy Rule cannot be combined, and the provision of treatment or payment, enrollment in a health plan, or eligibility for benefits may not be conditioned on receipt of an authorization unless the treatment is research-related. HHS now proposes limited exceptions for research authorizations whereby covered entities would be permitted to combine conditioned and unconditioned authorizations (forming "compound" authorizations) presented for research purposes, provided that the authorizations clearly denote which, if any, research components are conditioned upon receipt of authorization and clearly disclose the individuals' right to opt in to any unconditioned research activity.

In addition, HHS is seeking comment on whether and how the Privacy Rule could be amended to permit authorizations for future or secondary research uses of PHI. At present, authorizations may be valid only if the research is expressly described in the authorization, which can inhibit future or secondary research that may not have been fully formulated or anticipated at the time of the initial authorization. HHS has not proposed a specific modification to the Privacy Rule to accommodate the contemplated change, but rather is seeking comment on several options outlined in the proposed rules' preamble, such as whether a research authorization might be deemed adequate to cover future or secondary research when an individual could reasonably expect such future or secondary uses based on the information provided.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

Disclosures of PHI Regarding Decedents

Historically, HIPAA did not distinguish between living individuals and decedents in restricting disclosures of PHI, with certain exceptions for disclosures to law enforcement, coroners, medical examiners, and funeral directors, and to organizations involved in organ or tissue procurement, transplant, banking, or donation. HHS has noted that the current regulations' restrictions on disclosures of PHI about decedents have hindered appropriate use of historical data and have hampered covered entities' ability to communicate with decedents' friends and relatives. To address these problems, HHS has proposed to loosen the restrictions as follows:

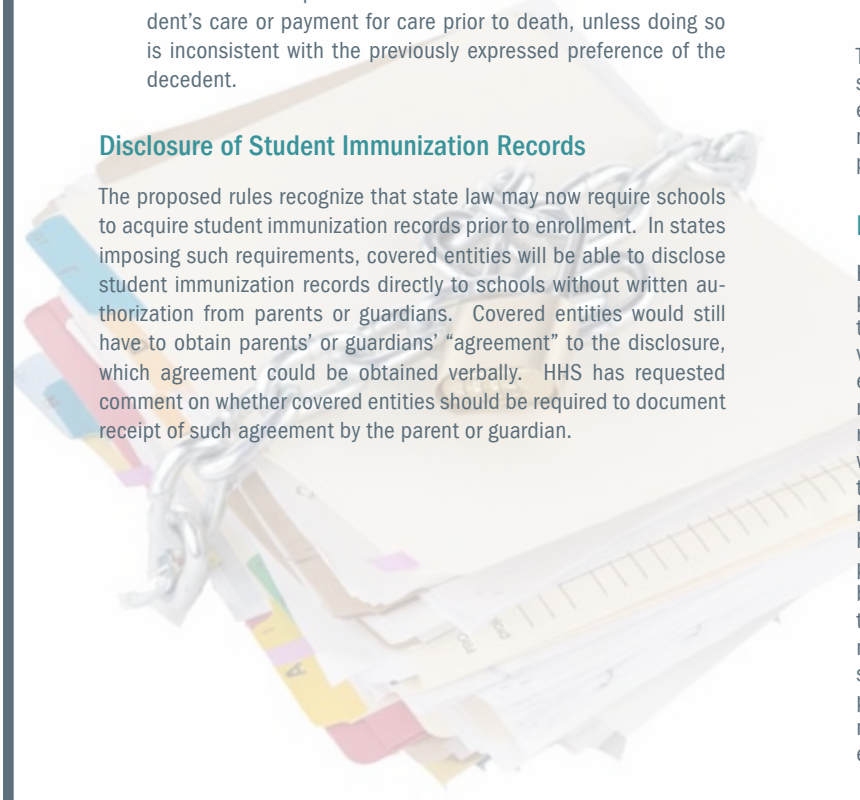
1. By providing that covered entities must abide by the requirements of the Privacy Rule with respect to a decedent's records only until the date that is 50 years from the date of the decedent's death;

2. By revising the definition of "individually identifiable health information" so that information regarding persons who have been deceased for more than 50 years will not constitute PHI (although HHS has only expressly discussed sunsetting the Privacy Rule's restrictions 50 years from the date of death, implementing this revision to the definition of PHI would effectively place the same duration on the requirements imposed by the Security Rule and the Breach Notice Rule, which requirements tie back to the definition of PHI); and

3. By permitting disclosures of PHI to family members, or to other relatives or close personal friends who were involved in the decedent's care or payment for care prior to death, unless doing so is inconsistent with the previously expressed preference of the decedent.

Disclosure of Student Immunization Records

The proposed rules recognize that state law may now require schools to acquire student immunization records prior to enrollment. In states imposing such requirements, covered entities will be able to disclose student immunization records directly to schools without written authorization from parents or guardians. Covered entities would still have to obtain parents' or guardians' "agreement" to the disclosure, which agreement could be obtained verbally. HHS has requested comment on whether covered entities should be required to document receipt of such agreement by the parent or guardian.



New and Revised Provisions Related to Privacy Notices

Amendments to Notice of Privacy Practices

Several of the changes proposed by HHS will necessitate corresponding changes to notices of privacy practices, namely the following:

1. The notice must describe uses and disclosures requiring an authorization, which will include sales of PHI, uses or disclosures of PHI for marketing, and uses or disclosures of psychotherapy notes (see above categories entitled "Use of PHI for Marketing" and "Sale of PHI");

2. The notice must describe uses and disclosures of PHI for fundraising, but in addition the individual's right to opt out of such uses and disclosures must be described (see above category entitled "Use of PHI for Fundraising");

3. If the covered entity intends to send treatment communications in exchange for financial remuneration, the notice must disclose that fact and describe the individual's right to opt out of such communications (see above category entitled "Use of PHI for Treatment Communications"); and

4. The notice must describe the individual's right to request restrictions of disclosures to health plans for payment or health care operations regarding services for which the individual has paid in full out of pocket (see above category entitled "Requests to Restrict Disclosures of PHI When Paid Out of Pocket").

The first three categories listed above must be described in separate statements within the notice of privacy practices. Covered entities not engaging in any of the activities that are the subject of these revised notice requirements may not need to update their notice of privacy practices.

Redistribution of Notice of Privacy Practices

HHS has clearly stated that the above-described changes to notices of privacy practices will each constitute a material change to the notices, thereby triggering the Privacy Rule's requirement to redistribute the revised notices. For non-health-plan covered entities, this will usually entail posting the revised notice in prominent locations, making the revised notice available to individuals upon request, and providing the revised notice rather than the former notice at the time of initial contact with new patients or customers. HHS has stated that this obligation to redistribute notices is not overly burdensome for providers. HHS has stated, however, that the redistribution requirements imposed on health plans (which necessitate that the plan actively notify participants within 60 days of making any material change to the notice) may be overly burdensome and solicits comment on revising the redistribution requirements applicable to health plans. HHS has advanced a number of proposed options on which it specifically requests comment, such as replacing the 60-day requirement with a requirement for health plans to redistribute revised notices only in their next annual mailing to members such as at the beginning of the plan year or during the open enrollment period.

New and Revised Provisions Related to Business Associates

Additional Types of Entities Designated "Business Associate"

The proposed rules expand and clarify the definition of "business associate" to include:

1. Subcontractors of business associates that create, receive, maintain, or transmit PHI on behalf of the business associate;
2. Vendors of personal health records acting on behalf of a covered entity;
3. Organizations transmitting PHI on behalf of a covered entity, such as Health Information Organizations and E-Prescribing Gateways, assuming they require routine access to PHI (acting as a "conduit" with only random and infrequent access will not trigger the definition); and
4. Patient Safety Organizations (as defined by the Patient Safety and Quality Improvement Act of 2005).

Business Associate Privacy Requirements

Business associates are prohibited from using or disclosing PHI other than in accordance with the provisions of their business associate agreements, as required by law, or as needed for certain of their own business functions. Business associates also may not disclose PHI in a manner that would violate the Privacy Rule if done by the covered entity. (As such, the new proposed restrictions on certain uses and disclosures of PHI, described above, are relevant to business associates.) While these provisions were historically made part of business associate agreements (as required by the current Privacy Rule), the proposed rules now make the Privacy Rule's requirements direct obligations (rather than contractual obligations) of the business associate. In addition, business associates now have a direct obligation to abide by the "minimum necessary" standard.

Under the proposed rules, business associates would be expressly required to disclose PHI in the following circumstances:

1. When required by HHS as part of an investigation to determine the business associate's compliance; and
2. To the covered entity, the individual to whom the PHI pertains, or that individual's designee in response to an individual's request for an electronic copy of PHI (a new individual right described in the above category entitled "Access to Electronic Protected Health Information").

(Note: Subcontractors meeting the new definition of business associate will also have to meet these same compliance obligations.)

Business Associate Security Requirements

The entire Security Rule now applies directly to business associates, including the provisions regarding evaluation of the reasonableness of addressable implementation specifications and other provisions related to implementation of the substantive security requirements. While this change is easy to articulate, actual implementation will be daunting for most business associates, which may not appreciate the detailed and comprehensive nature of the provisions set forth by the Security Rule. The Security Rule mandates, for example, several required elements including: periodic risk analyses; sanction policies; information system activity review (such as system logging and monitoring); procedures to authorize, supervise, modify, and terminate workforce access to ePHI; information access management procedures; training; incident response procedures; data backup plans; contingency plans; disaster recovery plans; periodic program evaluations; facility access controls; workstation security; portable media controls; emergency access procedures; unique user IDs; audit controls; integrity controls; and appropriate written agreements with contractors (see category below entitled "Amendments to Business Associate Agreements").

Multiple other "addressable" controls also are listed, and will be deemed required unless the business associate engages in a mandatory process to evaluate the control and whether it is appropriate to the organization, in light of several factors specified by the Security Rule. As is presently the case for covered entities, that process and the outcome must be documented and compensating controls must be implemented in order for business associates to decline implementation of "addressable" safeguards.

(Note: Subcontractors meeting the new definition of business associate will also have to meet these same compliance obligations.)

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

Business Associates Directly Liable for Violations

Prior to the HITECH Act, business associates were not directly liable under HIPAA but rather were liable to the extent provided by their business associate agreements or other contracts with covered entities. Under the proposed rules, business associates are directly required to abide by certain Privacy Rule restrictions and all Security Rule requirements, and they also are directly liable for violations of those provisions.

(Note: Subcontractors meeting the new definition of business associate will also face this direct liability.)

Covered Entity Liability for Business Associates

While the proposed rules render business associates directly liable for HIPAA violations, as described above, this proposal also would cause covered entities to lose the benefit of an exception that previously allowed them to avoid liability for the actions of business associates acting as agents if:

1. The relevant contract requirements had been met;
2. The covered entity did not know of a pattern or practice of the business associate that violated the contract; and
3. The covered entity did not fail to act with regard to those violations.

With this change, covered entities could be held liable for the acts or omissions of business associates who are agents, or even if the appropriate contractual measures were in place and the covered entity did not know of violations by the business associate. That possibility raises the stakes for covered entities and exacerbates the need to conduct appropriate diligence on business associates, a need that was already heightened by the increased penalty amounts and breach notification obligations, both imposed by earlier rulemakings.

Amendments to Business Associate Agreements

In addition to retaining much of the previously required contract language, HHS proposes to require amendment of business associate agreements to expressly provide:

1. To the extent the business associate will carry out a covered entity's obligation under the Privacy Rule, that the business associate will comply with the requirements of the Privacy Rule that would apply to the covered entity in its performance of the obligation;
2. That the business associate will comply with the applicable requirements of the Security Rule;
3. That the business associate will require subcontractors that create, receive, maintain, or transmit ePHI on behalf of the business associate to enter into a contract in which the subcontractors agree to comply with the applicable requirements of the Security Rule; and
4. That the business associate will report to the covered entity any security incident of which it becomes aware, including any breaches of unsecured PHI.

Any existing business associate agreement that complies with current HIPAA requirements and is not renewed or modified during the time that is 60 to 240 days after publication of the final rule will be presumed compliant until the earlier of:

1. The date the contract is renewed or modified on or after the date that is 240 days from publication of the final rule; or
2. The date that is one year and 240 days from the date of publication of the final rule.

New and Revised Provisions Related to Subcontractors

Subcontractors as Business Associates

Subcontractors that meet the new definition of "business associate" will now face the same compliance obligations and potential liability as do business associates (see section above regarding changes affecting business associates).

Implementation of Subcontractor Agreements by Business Associates

Business associates will now have an express obligation to implement contracts with their subcontractors (the current requirement is simply to ensure that the subcontractors "agree" to the same obligations imposed on the business associate, but a contract was not expressly required). That contract would essentially mirror the business associate agreement.

Business Associates Demanding Cure of Contractual Violations by Subcontractors

Under current requirements, covered entities must demand cure of contractual violations if they know of a pattern or practice of activity by a business associate that would constitute a material breach or violation of the business associate agreement. Following a cure period, if the breach or violation had not ended, the covered entity was required to terminate the agreement or report the violation to HHS when terminating the contract would be infeasible. While the proposed rules continue to require termination of the agreement in the absence of cure, they eliminate the duty to report to HHS. In addition, a parallel requirement has been imposed for business associates, who must similarly terminate their agreements with subcontractors in the event the business associate knows of a pattern or practice of activity by the subcontractor that would constitute a material breach or violation of the agreement, and the subcontractor has failed to cure the violation.

New and Revised Provisions Related to Enforcement

Previous revisions to the Enforcement Rule changed the annual maximum civil penalty for HIPAA noncompliance from $25,000 per violation to $1.5 million per violation, a 60-fold increase. Changes to the Enforcement Rule contained in this rulemaking clarify a number of key provisions, including the following:

1. References to business associates are included throughout in order to effectuate business associates' direct liability for HIPAA violations (see above category entitled "Business Associates Directly Liable for Violations").
2. In keeping with the HITECH Act's mandate that HHS must audit compliance, a revision is proposed to state that HHS "will" investigate complaints and conduct compliance reviews (the current wording provides that the agency "may" do so).
3. Compliance reviews by HHS will be mandatory when a review of the facts indicates possible incidents of "willful neglect," even if no complaint has been received.
4. HHS will no longer be required to resolve cases of willful neglect by informal means, but may do so if it chooses.
5. HHS proposes giving itself the right to disclose PHI for law enforcement purposes in order to facilitate enforcement actions by (or in cooperation with) state attorneys general or other federal agencies such as the Federal Trade Commission.
6. HHS proposes additional factors that it may consider in determining the amount of a civil penalty, key among them the addition of reputational harm as a factor (reputational harm also must be considered in determining whether a security breach is reportable under the current Breach Notice Rule).

The proposed rules also modify the definition of "reasonable cause" in order to more clearly delineate penalty tiers. "Reasonable cause" will mean "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect." Accordingly, the penalty tiers will apply in the following degrees:

1. Violations of which the alleged violator did not know and would not have known by exercising reasonable due diligence ($100-$50,000/violation, up to an annual maximum of $1.5 million/violation);
2. Violations due to "reasonable cause" as defined above, rather than willful neglect ($1,000-$50,000/violation, up to an annual maximum of $1.5 million/violation); and
3. Violations due to willful neglect ($10,000-$50,000/violation, up to an annual maximum of $1.5 million/violation if the violation was corrected in a 30-day period running from the day the covered entity or business associate knew of the violation or would have known of it by exercising reasonable diligence; absent correction in that 30-day period the penalty is $50,000/violation up to an annual maximum of $1.5 million/violation).

About the Author

Elizabeth Johnson's practice focuses on privacy, information security, and records management. Her comprehensive, practical approach to privacy law is reflected by the diversity of her clients, which hail from a variety of industries including health care, financial services, insurance, retail, telecom, utility, technology, consumer goods, and client services. Elizabeth has also worked with organizations of various size and scope, ranging from Fortune 100 companies with international reach to local charities. She was listed among the top privacy professionals in Computerworld's "2008 Best Privacy Advisors" report. Elizabeth may be reached at 919.783.2971 or ejohnson@poynerspruill.com.

Kim Licata, Of Cousel to the firm's Raleigh office, assisted with this article. She has advised health care providers and facilities on regulatory and compliance issues for over thirteen years. Her practice is designed to take the legal worry out of business ideas and assist her clients in actualizing their goals. Kim prides herself on being accessible and creative in her approach to complex situations. In addition to her regulatory work, Kim has years of litigation experience that make her a well-rounded advocate for her clients, understanding the true legal and litigation risks faced by health care entities and offering sound, practical legal advice. She may be reached at 919.783.2949 or klicata@poynerspruill.com.