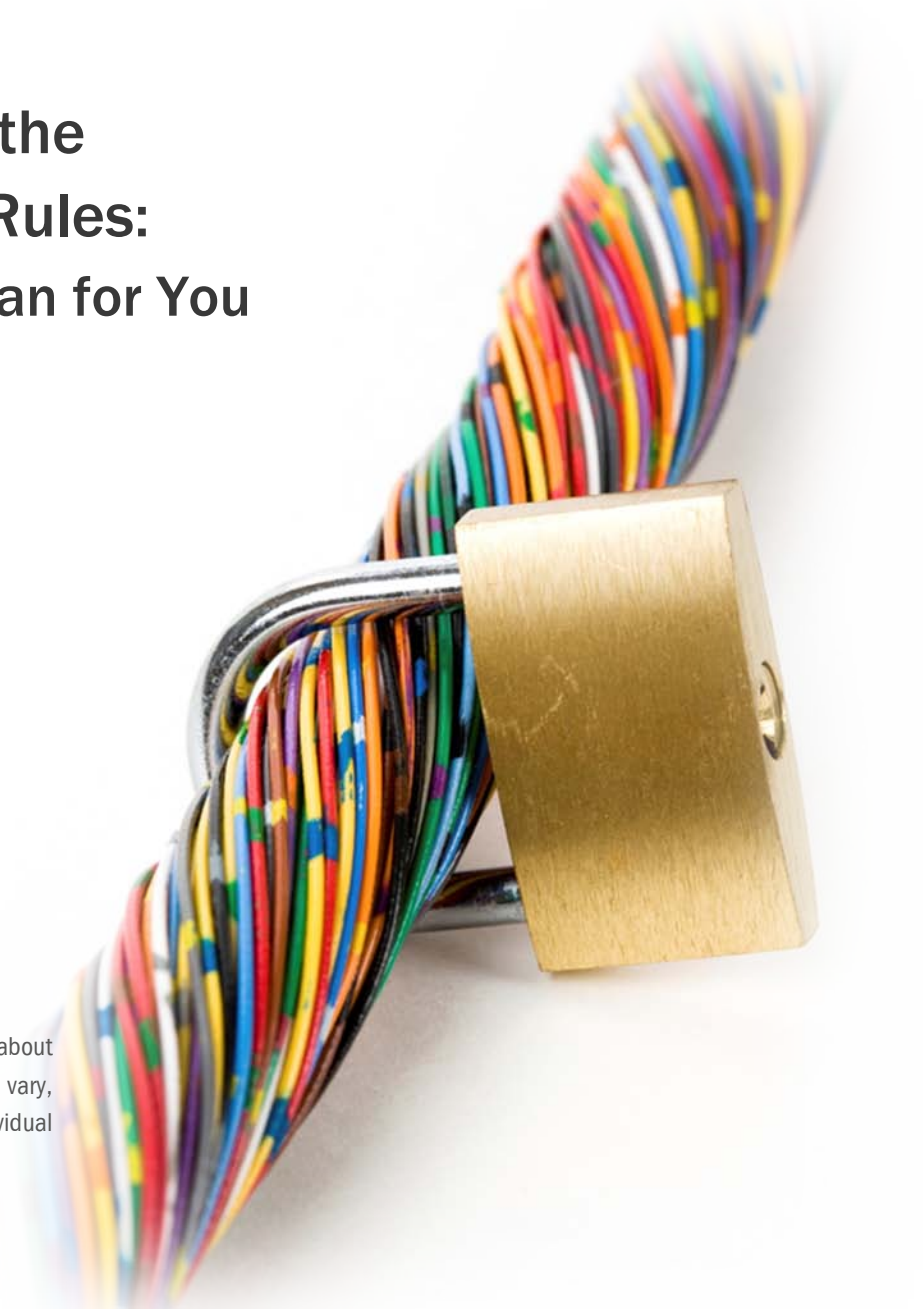
Poyner Spruill LLP
ATTORNEYS AT LAW

A Comprehensive Summary of the Final Omnibus HIPAA/HITECH Rules:

Key Provisions and What They Mean for You

By Elizabeth Johnson
919.783.2971
ejohnson@poynerspruill.com
@PoynerPrivacy



EXECUTIVE SUMMARY

On January 25, 2013, the Federal Register will publish final omnibus rules written by the U.S. Department of Health and Human Services (HHS) to modify the HIPAA Privacy, Security, Breach Notification and Enforcement Rules. The modifications implement most of the privacy and security provisions of the HITECH Act and relevant provisions of the Genetic Information Nondiscrimination Act. While some of the rule changes are not surprising, others are very impactful and will markedly change the obligations imposed on covered entities, business associates and subcontractors. Some of the more significant provisions are described here, and a comprehensive review of all the key changes is provided following this summary. Please feel free to contact us with questions.

Important Deadlines

The compliance deadline for virtually every provision of these rules is September 23, 2013. A longer period is provided where updates to existing business associate and data use agreements are required; those agreements may not need to be updated until September 22, 2014 provided they are not modified or renewed prior to that date.

Breach Notification

HHS has eliminated the harm threshold that provided notice of a security breach would only be required if the breach posed a significant risk of harm to affected individuals. It has provided instead that **any** use or disclosure of protected health information (PHI) that is not permitted by the Privacy Rule will be **presumed** to be a reportable breach. Covered entities and business associates can defeat this presumption by conducting a risk analysis using factors articulated by HHS, but the agency has made clear its expectation that impermissible uses and disclosures of readily accessible PHI will likely be a reportable breach. This change will mean an increase in the number of breaches reported.

Business Associates

Much of the Privacy Rule and all of the Security Rule now apply directly to business associates and their subcontractors. Business associate agreements are likely to require updates and, in light of breach requirements and increasing compliance reviews, covered entities should enhance their efforts to review business associate compliance and consider appropriate liability protections in their business associate agreements.

Enforcement and Penalties

HHS has retained the high penalty structure currently in effect, meaning that penalties can range from $100 to $50,000 per violation depending on culpability, up to an annual maximum cap of $1.5 million on a per provision basis. Business associates and subcontractors are directly liable for their violations, but covered entities also can be penalized for their violations. HHS is now required to conduct compliance reviews if willful negligence is indicated following a preliminary review of the facts.

Privacy Requirements

The final rules address multiple privacy issues related to uses and disclosures of PHI, such as communications for marketing or fundraising, exchanging PHI for remuneration, disclosures of PHI to persons involved in a patient's care or payment for care, and disclosures of student immunization records. In addition, individuals have new rights to restrict certain disclosures of PHI to health plans and to request access to electronic PHI (ePHI). Notices of privacy practices, research authorizations, internal policies, and training programs may require updates to address the rule modifications.

Security Requirements

Business associates and subcontractors must comply with the Security Rule in full. Given the complexities of achieving Security Rule compliance, business associates and subcontractors should begin efforts now to meet the September 23 compliance deadline.

Genetic Information

To implement the Genetic Information Nondiscrimination Act, HHS has included "genetic information" as a type of health information subject to HIPAA rules, and has imposed restrictions that will prohibit health plans from using genetic information for underwriting purposes.

As with most regulations, the details matter, so we have provided a more comprehensive summary of all the substantive requirements and described in brief how they will impact the regulated community from a practical standpoint. Please contact us with any questions, and you can sign up for other privacy and information security updates here.

IMPORTANT DATES AND GENERAL APPLICATION OF RULES

Deadlines

Key Provisions	What the Provisions Mean for You
• The effective date of these rules is March 22, 2013. • The compliance date is 180 days later on September 23, 2013. • A deferred compliance date is provided in certain cases for existing business associate agreements (refer to section regarding Business Associate Contracting). At the latest, all of these contracts must be compliant by September 22, 2014. • OCR has included in the final rules a "default" compliance period of 180 days for future HIPAA Rule modifications.	• Covered entities and business associates will not have as much time as they might have hoped to implement these new measures. That will be problematic for any business associates that have not started working on implementation, particularly Security Rule compliance. • Unless otherwise stated explicitly, all of these HIPAA rule changes and all *future* HIPAA rule changes will require compliance within 180 days of the effective date, which by law is the very minimum time HHS is required to provide as a compliance period. Going forward, the regulated community can assume it will usually have about 6 months to comply with new requirements.

General Application of Rules

Key Provisions	What the Provisions Mean for You
• Numerous rule provisions have been applied directly to business associates and their subcontractors (refer to section regarding Business Associates for additional details). • The final rules require that hybrid entities include all of their business associate functions within their designated health care components, such that the health care components are responsible for the full HIPAA compliance of their business associate functions.	• If your organization carries out some HIPAA covered functions and some non-HIPAA covered functions, it is a hybrid entity within the meaning of the rules. Examples of hybrid entities include academic medical centers, which teach students (not HIPAA covered) and treat patients (HIPAA covered), and retailers that sell groceries (not HIPAA covered) and fill prescriptions (HIPAA covered). Within these organizations, there are business units that perform business associate-like support functions, such as the IT or Legal Departments. HIPAA permits hybrid entities to designate which "components" of its business are HIPAA covered and, once documented, only those designated components have to comply with HIPAA. Under the current rules, hybrid entities may, but do not have to, also designate their business associate-like business units as part of the HIPAA covered health care components. Under the final rules, once effective, covered entities will be strictly required to include their business associate-like business units within their designated health care components. As such, internal departments that provide support functions to health care components must comply with HIPAA due to their business associate-like activities, just as legally-separate entities that are business associates now have to comply with many provisions of the rules. • Feeling confused about the explanation above? Don't think too hard – any parts of your organization that act like covered entities need to comply with HIPAA, and any parts of your organization that provide services and support to those business units, and also access PHI, will likewise need to comply with HIPAA.

BREACH NOTIFICATION

Notification Standard

Key Provisions	What the Provisions Mean for You
• HHS has eliminated the "harm threshold" for breach reporting. Under the prior rule, breaches were not reported unless they posed a "significant risk of reputational, financial or other harm" to individuals. Under these final rules, the determination of whether an incident is a breach depends not on the likelihood affected individuals might be harmed, but rather on the risk that PHI has been "compromised." An incident is presumed to be a breach unless a risk analysis reveals a "low probability" that PHI has been compromised. • The requisite risk analysis must include at least the following factors: o The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; o The unauthorized person who used the PHI or to whom the disclosure was made; o Whether PHI was actually acquired or viewed; and o The extent to which any risk to PHI has been mitigated. • Under the interim final rule, incidents affecting PHI would not constitute a breach if certain identifiers listed by the rule were not implicated (a limited data set less dates of birth and zip codes). That exception has been removed from the final rules. Instead, the question of whether the PHI affected is individually identifiable will factor into the risk analysis. • HHS has retained "safe harbors" for PHI that is encrypted or disposed of securely.	• Until the compliance date of these final rules (September 23, 2013), security breaches are to be reported as required by the agency's current rule on this topic (which applies or "significant risk of harm" standard). After the compliance date, covered entities and business associates should conform to these final rules when evaluating incidents and assessing their breach notification and response obligations. • Incidents that violate the Privacy Rule, that do not meet one of the provided exceptions, and that are not subject to a safe harbor (see below) are presumed to be breaches. To defeat that presumption, covered entities and business associations must evaluate the incident using the risk analysis approach outlined by the final rules. Notification will be required if the risk analysis reveals there is greater than a "low probability" that the PHI will be or has been compromised. • Be aware that all reported breaches are, by definition, describing use or disclosure of PHI that violated the Privacy Rule. As such, when you notify of a breach you are also self-reporting a HIPAA violation. If the notice suggests willful negligence by the covered entity or business associate, then HHS is required to investigate. • The agency states that impermissible uses of PHI, and not only impermissible disclosures, are potentially subject to breach notification. • Much of the remaining provisions of the breach notification requirements remain the same as were provided in the interim final rule, including: o The same exceptions to the term "breach" are provided and address limited circumstances when: PHI could not reasonably be retained; PHI is accessed inadvertently by a covered entity or business associate's workforce member unintentionally and in good faith; and an inadvertent disclosure is made by a person at the covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate (or at an organized health care arrangement in which the they participate). In each case, further impermissible use, or disclosure of, PHI would render the exceptions inapplicable. o Notification provisions remain the same, including requirements for covered entities to notify affected individuals, HHS and, in some cases, the media. As was the case in the interim final rule, breaches affecting 500 or more individuals must be notified to HHS contemporaneous with the provision of notice to individuals, whereas breaches affecting less than 500 individuals can be logged and reported to HHS on an annual basis. Business associates that discover a breach must notify covered entities, and subcontractors must notify business associates who then notify covered entities. o HHS continues to provide a safe harbor from breach notification requirements for PHI that is encrypted or disposed of in keeping with its earlier guidance on the topic. Encryption will continue to be a critical tool in minimizing the risk of breach reporting.

Notification Standard

Key Provisions	What the Provisions Mean for You
	o Notifications are still required without unreasonable delay and in no case later than 60 days from the date the breach is discovered. The rule continues to allow notification delays if law enforcement advises that notification might impede their investigation. • The risk analysis now required by the final rules must be documented and retained to meet the covered entity's burden of proof to demonstrate that unreported incidents did not rise to the level of a "breach." • We expect the elimination of the harm threshold to markedly increase the number of breaches reported to HHS. The agency reports that it already receives approximately 19,000 breach notifications annually, about 250 of which affect more than 500 people. OCR estimates about 6.71 million people are affected by these breaches annually. With these rule changes, that number will go up, but will also motivate covered entities and business associates to pursue safe harbors like encryption and redouble efforts to comply with these rules to prevent breaches. • If you had not considered it already, now would be a good time to start comparison shopping for insurance policies that cover breach response and notification costs (but read the fine print and seek counsel on the scope of coverage and policy details. • For additional insights on the effect of this change and how you can prepare, please review our article, Brace for Impact – Final HITECH Rules Will Require Substantially More Breach Reporting (visit www.poynerspruill.com and click on Publications).

"Now would be a good time to start comparison shopping for insurance policies that cover breach response and notification costs."

BUSINESS ASSOCIATES

Who Are Business Associates?

Key Provisions	What the Provisions Mean for You
• A business associate is, and continues to be, an entity that performs functions, activities or services on behalf of covered entities that involve use or disclosure of PHI. HHS has modified the rules to provide that business associates may "create, receive, *maintain*, or transmit" PHI, clarifying that entities merely storing PHI also are business associates. Lack of a contract between the parties will not prevent this designation.	• Business associates will need to bring their subcontractors into the loop by asking them to execute appropriate HIPAA contracts (a.k.a., business associate agreements). While that should have occurred under current rules, the requirement is not explicit. Motivation to do so should be high since business associates can now be held directly liable for any failure in this regard.
• Subcontractors of business associates are, by definition, now considered business associates if they create, receive, maintain or transmit PHI. Lack of a contract between the parties will not prevent this designation.	• Whether a subcontractor is a business associate will be decided based on the nature of their activities. Subcontractors that provide services in a manner that fits the definition of business associate will themselves be business associates. That outcome cannot be avoided merely by forgoing a contract.
• HHS has clarified that organizations providing personal health records (PHRs) on behalf of covered entities are business associates.	• PHR providers sometimes claim they are "conduits" for PHI and their access to PHI does not render them business associates. That claim was dubious before, and is clearly unsupportable now given the guidance provided by the agency in the final rules' preamble, and its decision to exclude PHR providers from the list of entities characterized as merely transmitting PHI on behalf of covered entities (such as E-Prescribing Gateways). PHR providers are, however, only business associates if they act *on behalf of* covered entities. PHR providers that provide services directly to patients and other individuals do not become business associates simply because they receive PHI directly from a covered entity, such as pursuant to an individual authorization. If a PHR provider works on behalf of both a covered entity and individual patients, then HHS confirms that the PHR provider is only a business associate when it acts on behalf of the covered entity.
• Health Information Organizations (which include health information exchange organizations), E-Prescribing Gateways, and others entities that transmit PHI on behalf of covered entities are business associates if they access PHI on a "routine basis."	• With regard to the "conduit exception," HHS states that access on a "routine basis" will be determined by the facts, but reminds us that the conduit exception is narrow and intended to exclude only courier services, such as the U.S. Postal Service, UPS and "electronic equivalents" such as internet service providers (ISPs), which may include temporary storage. For entities that transmit data or records, "occasional, random" access to PHI will not cause them to be deemed business associates *unless* their access is necessary to the performance of their services to the covered entity. Providing services like record locator services and oversight and governance functions are likely to be considered more than "random" access by HHS, and would likely render the provider organization a business associate.
• Patient safety activities have been added to the list of functions that may cause an organization to be deemed a business associate if done on behalf of a covered entity.	• HHS confirms that records storage services and others that store PHI are business associates, and are not subject to the "conduit exception" which is available only to those that act to transmit PHI. "Persistent" storage services, even without routine access to PHI, will cause a provider of those services to be a business associate. In the rules' preamble, HHS describes the need for a "shredding company" to comply with HIPAA, meaning that shredding and other disposal companies also are apparently considered business associates, even though their storage of records is likely to be temporary rather than persistent.
• HHS confirms that researchers may be business associates if they perform a service for covered entities, such as de-identifying PHI or creating a limited data set, even if the de-identified PHI or limited data set is created for the researchers' own use.	• HHS confirms that Patient Safety Organizations are business associates when they engage in activities like quality analysis on behalf of covered entities.

New Requirements for Business Associates

Key Provisions	What the Provisions Mean for You
• Numerous provisions of the rules now expressly apply to business associates (and their subcontractors). These include: o All applicable provisions of the Security Rule; o The use and disclosure limitations of the Privacy Rule, including the minimum necessary principle and, if applicable, de-identification standards; o The requirement to provide a copy of ePHI to a covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement); o The requirement to maintain an accounting of disclosures; and o The obligation to provide PHI to HHS during an investigation or compliance review.	• Business associates and their subcontractors have nine short months to become compliant with these final rules. HIPAA requires dozens of documented policies and procedures, as well as time-consuming implementation of technical requirements, like conducting a security risk analysis and developing a mitigation plan, producing a contingency plan, potentially encrypting ePHI, and preparing systems to log and monitor user activity. Once implemented, compliance also necessitates training your workforce on the full program, and that training also must be documented. In order to satisfy contracting requirements, you will need to identify all service providers that access PHI and request that they execute appropriate business associate agreements. Because so much work is required, if you had not already started, you may find that the nine months HHS has provided is not adequate to fully comply prior to the compliance deadline. • Given that covered entities can be held liable for their business associates' noncompliance, business associates should expect to get more attention from their covered entity clients, including increased diligence, security reviews, and full blown audits. If you are a covered entity and you have not already undertaken these activities with your business associates, it is time to start.

Contracting with Business Associates

Key Provisions	What the Provisions Mean for You
• Covered entities are still required to contract with their business associates, but are not required to contract directly with their business associates' subcontractors. • Business associates are required to have business associate agreements in place with their subcontractors, including certain provisions prescribed by the rules. • As described in detail above, many more entities are considered business associates (including subcontractors) and all of them must have a business associate agreement in place.	• The final rules necessitate a review of your business associate agreements, even if you already made updates in anticipation of these rule changes based on proposals published earlier. Although most of the *concepts* advanced in these final rules are very likely captured in existing business associate agreements, those contracts are unlikely to capture *exactly* the provisions HHS is now mandating so any organizations wishing to strictly adhere to the agency's requirements will want to modify their contracts accordingly. • Additional updates are advisable if your contracts do not speak to increased business associate compliance obligations, described above, which include many substantive provisions of the Privacy Rule and all of the Security Rule. Enhanced provisions are also warranted regarding security breach response and reporting and carrying out obligations related to individuals' privacy rights, such as the right to receive copies of PHI. • Business associates may wish to update their agreements with covered entity clients to document their rights when they become aware of material noncompliance by those clients. Those rights are provided in the rules, so updates for this purpose are not strictly necessary, but failing to include them in agreements will deprive business associates of contract-based legal remedies in the event the issue arises.

Contracting with Business Associates

Key Provisions	What the Provisions Mean for You
• As provided by the HITECH Act, these rules confirm a business associate's rights and obligations if it knows of a pattern of activity or practice by a covered entity client that constitutes a material breach of the HIPAA Rules. These same rights and obligations also will extend to subcontractors. • Certain contracting provisions in the Security Rule were eliminated in order to avoid duplication of similar terms in the Privacy Rule. In addition, certain contracting provisions in the Privacy Rule were clarified to address breach reporting and Security Rule compliance. Business associate agreements also must specify that, to the extent a business associate is contracted to carry out a covered entity's HIPAA obligations, such as providing a privacy notice, the business associate must comply with the HIPAA Rules that would apply to the covered entity in the performance of such obligation. • The final rules provide the possibility of a longer compliance period for business associate agreement adjustments. Business associate agreements entered into before January 25, 2013 (the publication date of the rules) that are not modified between March 26 and September 23, 2013 will be deemed compliant with HIPAA Rules (assuming they comply with the currently effective version) until the earlier of the date they are next renewed or modified or September 22, 2014.	• As was already the case, business associates must report security breaches to covered entities, and covered entities are required to report breaches to affected individuals and HHS (and in some cases to the media). Business associates should expect to see provisions in proposed business associate agreements that go beyond the rules' assignment of responsibilities, including provisions that obligate the business associate to report the breach to affected persons and HHS directly, at the covered entity's discretion, and to pay costs associated with the breach and notification. • Given the increased penalties for noncompliance, and the prospect that covered entities can be held directly liable for business associate noncompliance, you can expect to see more negotiation and attention paid to provisions of business associate agreements that address limits of liability and indemnification. • Here's a breakdown of the compliance deadlines for business associate agreements (which includes agreements between business associates and their subcontractors): o Agreements newly entered into after January 25, 2013 must comply with the new provisions in the final rules. o Existing agreements that are renewed or modified on March 26, 2013 or thereafter must be brought into compliance with the final rules at the time of the renewal or modifications. o Agreements entered into before January 25, 2013 that comply with the current rules may be renewed or modified until March 25, 2013. If the parties do not wish to make further changes until absolutely required, they must avoid renewals or modifications on or after March 26, 2013 since any further adjustments would trigger an obligation to also bring the contract up to the standards articulated by these final rules. o Agreements entered into before January 25, 2013 that are not renewed or modified on March 26, 2013 or thereafter will be deemed compliant until September 22, 2014, on which date all business associate agreements must be modified to comply with these final rules.

Liability for Violations by Business Associates

Key Provisions	What the Provisions Mean for You
• Business associates can be directly liable for HIPAA noncompliance, meaning compliance reviews, fines, equitable relief and audits are all in play. • Since subcontractors of business associates are now also defined as "business associates" they also can also be directly liable for violations. • Covered entities are still directly liable for their business associates (if they constitute agents). Business associates are directly liable for their subcontractors (if they constitute agents). • If a covered entity and a business associate are both responsible for a violation, HHS can penalize both.	• Don't think too hard about who is liable for what. Everybody is liable for their own violations and their agents' violations. • Business associates will be subject to audits, compliance reviews, and enforcement actions by HHS as are covered entities. Same goes for their subcontractors. • Although business associates and their subcontractors, covered entities are not off the hook since they can be penalized for their agents' actions even if the agents were penalized directly. • HHS's new authority over business associates and subcontractors has multiplied many, many times over the potential enforcement targets the agency can pursue. Expect staffing increases and a continued uptick in the frequency and amount of monetary penalties. • HHS posits that a covered entity will not have an agency relationship with a business associate (nor a business associate with its subcontractor) if the covered entity does not have the ability to provide the business associate with ongoing instructions. If, by contrast, the covered entity has the ongoing authority to direct the business associate's authority, then HHS opines the business associate would be an agent of the covered entity. Where it can establish an agency relationship, HHS is free to hold the covered entity directly liable for the business associate's violations. It is common for business associate agreements to provide covered entities with exactly this type of ongoing authority to direct activities (such as providing that a business associate should only make PHI available to an individual at the covered entity's instruction). If, however, that ongoing ability to give direction causes the covered entity to be in an agency relationship with the business associate, and thus directly liable for the business associate's conduct, we may see business associate agreements drastically cutting back on the degree of a covered entity's ongoing authority to direct the business associate in an attempt to avoid that liability.

"Although it will be open season on business associates in terms of audits, compliance reviews, and fines, covered entities are not off the hook."

ENFORCEMENT AND PENALTIES

Compliance Reviews and Complaint Investigations

Key Provisions	What the Provisions Mean for You
• HHS is required to conduct compliance reviews and investigate complaints when a "preliminary review of the facts" suggests a violation due to "willful neglect" by the covered entity or business associate. The agency no longer has the option to disregard certain reported security breaches and individual complaints. The agency may choose to disregard (or pursue) apparent violations that are due to some lesser culpability than willful neglect. • HHS is no longer required to (but still may) attempt an informal resolution of noncompliance in lieu of formal enforcement.	• There will be many more compliance reviews and complaint investigations. Since the agency always requests copies of HIPAA policies in these reviews, it's definitely time to update your policy book. • Following a complaint, a reported breach, or similar incident, the agency may conduct an inquiry with the covered entity or business associate to gather additional facts to assess whether willful neglect or some greater culpability caused the violation. If so, the agency will be strictly required to conduct a compliance review. • Expect to see more formal investigations and settlement orders since informal resolution is no longer mandatory.

Fines

Key Provisions	What the Provisions Mean for You
• HHS may fine any covered entities, business associates and subcontractors that are responsible for a violation (it need not select only one party). • Violations are counted up "based on the nature of the…obligation to act or not act." New factors have been added to the fining calculus, including the number of persons affected by the violation and potential harm to those persons' reputations. • The agency states in the preamble to the rules that, generally, monetary penalties will be tallied on a per person and per day basis. The agency also notes that, in cases of a breach, there often will have been at least two violations: an impermissible use or disclosure of PHI and a safeguards violation. HHS may separately tally these violations when levying a monetary penalty.	• More fines and resolution payments (settlements) will fund more audits and enforcement. • There is no single definitive methodology for tallying monetary penalties. The agency retains discretion to add up fines based on a per person affected and per day basis, and also can take into account the nature of potential harms, such as limiting a person's ability to seek care or harming (or merely creating the potential to harm) their reputation or finances. Despite a lack of complete clarity as to how HHS tallies proposed monetary penalties, there is no doubt that the totals will be much larger than were possible prior to the HITECH Act. • If you discover a violation, correct it promptly and in no more than 30 days. Delaying beyond that timeframe will foreclose certain defenses that could decrease monetary penalty amounts. • HHS retains the authority to charge multiple violations related to a single event, such as a breach. As such, it is important to recall that the maximum annual cap of $1.5 million is applied on a "per provision" basis. It can still be multiplied several times over depending on the number of provisions violated. For example, violations of two different provisions could result in a total annual cap of $3 million, and violations of three provisions could result in a total annual cap of $4.5 million, and so on.

Fines

Key Provisions

- The agency has confirmed the higher penalty amounts it earlier issued in its interim final rule. This final rule retains the current penalty structure, which applies to violations that occurred prior to February 18, 2009.
- Certain defenses are provided, but vary depending on the date of the offense (those occurring prior to February 18, 2009 are subject to kinder treatment). Some of these defenses can be relied on only if violations are corrected within 30 days.

What the Provisions Mean for You

- The following chart summarizes the final monetary penalty system, which applies to violations that occur on or after February 18, 2009:

Degree of Culpability / "State of Mind"	Potential Penalty Per Violation	Maximum Annual Cap for All Violations of Identical HIPAA Provision
Violation was not known and could not have been discovered with reasonable diligence	$100 – $50,000	$1,500,000
Reasonable cause for violation, not due to willful neglect	$1,000 – $50,000	$1,500,000
Violation due to willful neglect, but corrected in 30 days	$10,000 – $50,000	$1,500,000
Violation due to willful neglect, not corrected in 30 days	$50,000	$1,500,000

"If you discover a violation, correct it promptly and in no more than 30 days. Delaying beyond that timeframe will foreclose certain defenses that could decrease monetary penalty amounts."

PRIVACY REQUIREMENTS

Scope of the Privacy Rule

Key Provisions	What the Provisions Mean for You
• Health information regarding a person who has been deceased for more than 50 years is excluded from the definition of PHI. • HHS has clarified that "provision of access to" PHI is a "disclosure" subject to HIPAA Rules. • Business associates are now directly required to comply with significant provisions of the Privacy Rule, and are expressly prohibited from using or disclosing PHI other than as permitted by their business associate agreements, and are prohibited from uses or disclosures of PHI that would not be permitted if done by their covered entity client. • Genetic Information is expressly included within the definition of "health information" and so will be subject to HIPAA Rules if it is individually identifiable.	• Persons long dead have no HIPAA privacy rights. The recently deceased are still covered. (Same goes for breach notification and security – not applicable to information about persons who have been dead more than 50 years.) However, state laws (such as those applicable to mental health and substance abuse records) and rules of professional responsibility may still apply. • Occasionally those faintly hoping to escape HIPAA's grasp will argue that there is no disclosure of PHI if the recipient has "view only" or "read only access." That position was baseless and is now officially dead with HHS's clarification of the definition of "disclosure" to expressly include access. This clarification also may result in more breach notifications if covered entities were construing mere viewing of PHI as not a disclosure and thus not a potential breach. • Covered entities should ensure that business associates comply with the applicable provisions of the Privacy Rule. That increased vigilance is advisable not only because covered entities can be directly liable for business associate noncompliance, but also due to enhanced breach notification requirements (covered entities must report breaches caused by business associates unless they contract otherwise) and the agency's enhanced fining authority. Business associates should undertake Privacy Rule implementation now and redouble any existing efforts to comply prior to the September 23, 2013 compliance deadline (refer to section regarding Business Associates for additional information). • Individually identifiable genetic information will be subject to Privacy Rule requirements (when handled by entities subject to HIPAA); that was a logical application of the rules prior to this modification, but now the agency has confirmed that HIPAA Rules apply to genetic information.

"Covered entities should ensure that business associates comply with the applicable provisions of the Privacy Rule. Increased vigilance is advisable not only because covered entities can be directly liable for business associate noncompliance, but also due to enhanced breach notification requirements."

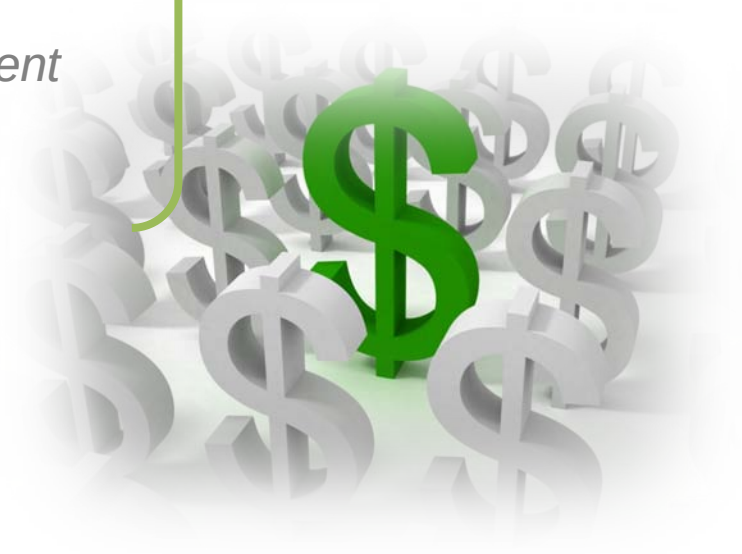
Marketing and Treatment Communications

Key Provisions	What the Provisions Mean for You
• The final rules provide that an individual's express authorization is required before a covered entity may make communication (see below for some exceptions) regarding treatment or health care operations where: o The covered entity receives financial remuneration from (or on behalf of) a third party in exchange for sending the communication; and o The communication is intended to encourage purchase or use of a product or service offered by the third party. • Communications that ***may*** be subject to this requirement include those regarding: o Appointment reminders; o Treatment reminders; o Alternative treatments; o Health care products or services. • Communications that are not subject to this requirement continue to include: o Face-to-face communications; o Promotional gifts of "nominal" value; o Refill reminders, adherence reminders, or other communications about a drug or biologic (or the generic equivalent) that is currently being prescribed for the individual, 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; o Communications about health in general, such as healthy living or encouraging routine diagnostic tests such as annual mammograms; o Communications about government or government-sponsored programs that benefit the public, such as eligibility for Medicare or Medicaid.	• The agency has markedly revised provisions related to marketing and treatment communications in comparison to the version of these rules it proposed in 2010. Citing confusion over the distinction between communications for "treatment" versus "health care operations," and confusion over the prior opt-in versus opt-out consent dichotomy it had proposed, the agency has now determined that a simpler, stricter policy is best. To that end, written communications that are intended to promote purchase or use of a third party's products or services will require prior individual authorization if the covered entity receives financial remuneration from or on behalf of that third party in exchange for sending the communication, with only a few exceptions. • In order to trigger this requirement, the financial remuneration received must have been provided in exchange for sending the communication. If a third party provides a covered entity with funds to implement a disease management program, for example, the covered entity may send communications encouraging participation in the new program without individual authorization because the payment it received from the third party was not paid in exchange for sending the communications. • The agency retained certain exceptions to the authorization requirement, such as for "in person" communications (including making written pamphlets available during in person patient visits). • All forms of communication that are not conveyed "in person" may be subject to these requirements, including those conducted by phone, fax, mail, electronic mail and text message. Please note that other federal and state laws may also apply to commercial messages of this nature. • Communications about drugs or biologics currently prescribed to individuals can be made without authorization even if some financial remuneration is paid to the covered entity, but only if the payment is "reasonably related" to the cost of making the communication. HHS has clarified that it considers such costs to include only labor, supplies and postage related to the communication. The payment cannot cover costs unrelated to the communication nor can it provide even a marginal profit. • HIPAA mandates a certain form and content for valid authorizations that should be followed here. The final rules also require covered entities to disclose in their marketing authorizations that they are receiving financial remuneration in exchange for sending marketing communications. • The final rules do not require that the communications themselves include an opt-out mechanism. Rather, the initial authorization would advise individuals of their right to revoke that authorization, as is required by HIPAA for all valid individual authorizations. Please note that other federal and state law also may apply and could require inclusion of an opt-out mechanism.

Marketing and Treatment Communications

Key Provisions	What the Provisions Mean for You
• "Financial remuneration" continues to mean "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.) This term includes payments made directly to a business associate who will carry out the communication on behalf of the covered entity. It does not include the receipt of in-kind or other non-financial benefits.	• Covered entities should evaluate the types of communications they send to patients, and specifically whether they receive any monetary compensation in exchange for sending them. If so, no further communications of this kind can be sent (after the compliance deadline of September 23, 2013) until the individual has completed an authorization providing consent for the communication. Covered entities may delegate this task to a business associate but, in either case, will need to track receipt of these authorizations. Because individuals can revoke authorizations, covered entities also will want to track any subsequent opt outs that indicate an individual no longer wants to receive subsidized health care communications.

"The final rules prohibit the sale of PHI unless the individual has authorized it. The authorization must expressly disclose that the covered entity will receive remuneration in exchange for PHI. A disclosure of PHI will qualify as a 'sale' if a covered entity or business associate receives remuneration, financial or otherwise, directly or indirectly, from or on behalf of the recipient in exchange for the PHI."



Sale of PHI

Key Provisions	What the Provisions Mean for You
• The final rules prohibit the sale of PHI unless the individual has authorized it. The authorization must expressly disclose that the covered entity will receive remuneration in exchange for PHI. • A disclosure of PHI will qualify as a "sale" if a covered entity or business associate receives remuneration, financial or otherwise, directly or indirectly, from or on behalf of the recipient in exchange for the PHI. Some exceptions are provided, such as disclosures for research purposes where the remuneration received represents a reasonable cost-based fee, or disclosures by business associates or their subcontractors, where the remuneration is provided by the covered entity or business associate respectively, and the remuneration is paid to compensate for the activities performed by the business associate or subcontractor. • Data use agreements in effect prior to January 25, 2013, pursuant to which the recipient receives a limited data set of PHI in exchange for remuneration, may continue until the earlier of September 22, 2014 or the date such agreements are next renewed or modified on or after September 23, 2013.	• Unlike provisions related to use of PHI for marketing, which apply only if communications are made in exchange for *financial* remuneration, the restrictions on sales of PHI apply if any form of remuneration, financial or otherwise, is received in exchange for PHI. • For the sales restriction to apply, the remuneration in question must be provided in exchange for the PHI rather than a product or service that results in the disclosure of PHI. In other words, the restriction does not apply where the disclosure of PHI is a "byproduct" of the arrangement, such as where a covered entity receives payment to perform activities, such as research. For example, HHS states in the rules' preamble that fees paid to a health information exchange are not considered to be remuneration paid in exchange for PHI; rather, the payment of those fees compensates the health information exchange for the services it provides, not the PHI itself. • By contrast, a sale of PHI will occur if a covered entity "primarily is being compensated to supply data it maintains in its role as a covered entity (or business associate)." As an example, HHS cites a circumstance in which a covered entity is paid by a researcher for a disclosure of PHI, and the payment exceeds a reasonable fee paid to cover the cost of preparing and transmitting the PHI. • In general, where this provision and other portions of the rules allow payment of reasonable, cost-based fees, the remuneration permitted can cover only direct and indirect costs to prepare and transmit the data, including labor, materials, and supplies, but not a profit margin. HHS states that it intends to issue guidance on this topic in the future. • HIPAA mandates a certain form and content for valid authorizations that must be followed if a covered entity wishes to sell PHI. The final rules also require covered entities to disclose in their authorizations that they are receiving remuneration in exchange for PHI. • Sales of limited data sets are subject to these restrictions, but HHS has provided something of a grace period for current exchanges of data occurring under an active data use agreement. Such disclosures may continue in exchange for remuneration until September 22, 2014 or until the time any modification or renewal of the data use agreement is undertaken after September 23, 2013, whichever is sooner. After that time the restrictions described herein will apply. If you do not already have a data use agreement in place, it's too late to implement one now and take advantage of this grace period; it only applies for agreements in place prior to January 25, 2013.

Fundraising Communications

Key Provisions	What the Provisions Mean for You
• The final rules clarify that a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following PHI for purposes of its own fundraising without an authorization: o Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth; o Dates of health care provided to an individual; o Department of service information; o Treating physician; o Outcome information; and o Health insurance status. • Each fundraising communication must include a "clear and conspicuous" opt-out mechanism that does not place an undue burden on the individual or impose more than a nominal cost. • A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications. • A covered entity's notice of privacy practices must describe the covered entity's intent to send fundraising communications and describe the individual's right to opt out (refer to section regarding Notice of Privacy Practices for additional information).	• The final rule provides a limited set of circumstances in which a covered entity can use and disclose certain PHI for fundraising without an authorization. If covered entities wish to make broader uses or disclosures of PHI for fundraising, they may do so with a valid authorization. • Whether or not an authorization was required or was obtained to support fundraising, covered entities must provide an opportunity to opt out in each subsequent fundraising communication. Covered entities may provide individuals with an opportunity to opt back into fundraising communications in the future. • HHS supports but does not mandate use of a toll free number or email-based mechanism to provide individuals with the opportunity to opt out of future fundraising communications. HHS believes that requiring individuals to send a letter in order to opt out would constitute an "undue burden," unless the individual has been provided with a pre-printed, postage-paid postcard. • The scope of the opt out is left to the covered entity, so if fundraising communications are clearly limited in scope to particular campaigns, so too can opt outs be of similarly limited scope. For example, a covered entity may send separate communications about opportunities to sponsor an event and a campaign to fund a new facility. The covered entity may choose whether the opt-out mechanism it provides in each communication is "global" in effect (opts individuals out of all future fundraising communications of any type) or rather is specific to a given fundraiser. If the opt out is to be limited in effect, that fact should be explicitly described in the opt-out language. If a covered entity chooses to use a limited opt out, it must be capable of tracking, managing and honoring these more specific opt outs to avoid inadvertent noncompliance. • HHS removed language from the Privacy Rule stating that covered entities must make only "reasonable efforts" to ensure that an individual who has opted out will not receive future fundraising communications. Accordingly, much less allowance will be made for covered entities that fail to timely honor an individual's stated preference to opt out of fundraising communications due to a reasonable oversight. • Although the HITECH Act refers only to written fundraising communications, HHS has chosen to apply these requirements to all fundraising communications, meaning phone calls placed for fundraising purposes must inform individuals of their right to opt out.

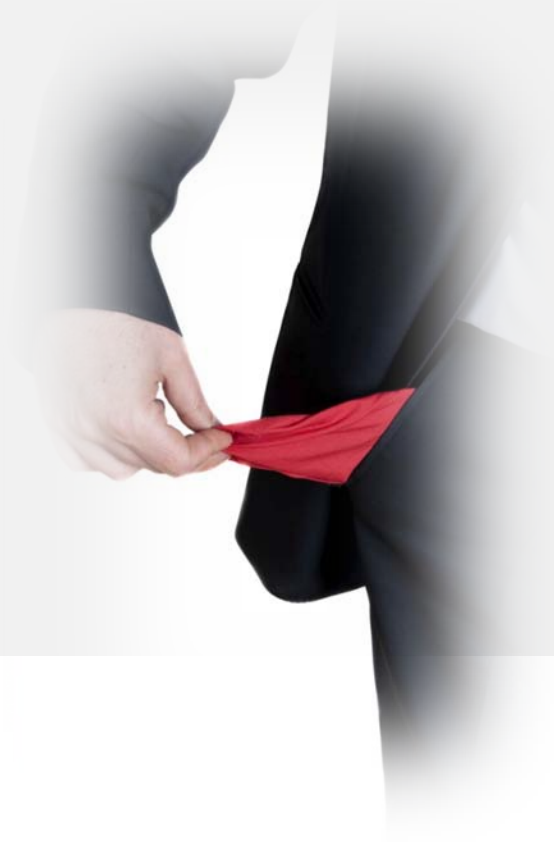
Individual Right to Request a Copy of PHI

Key Provisions	What the Provisions Mean for You
• The final rules confirm that individuals have a right to request copies of PHI in any form they choose, provided PHI is "readily producible" in that format. If the PHI requested is maintained electronically in one or more designated record sets, the covered entity will be required to produce an electronic copy of PHI if the individual requests it. • HHS has provided that covered entities must provide copies of PHI to other parties if designated by the individual. The individual's request must be written and signed, and must clearly identify the designated recipient and where to send the copy of PHI. • The final rules permit covered entities to charge a "reasonable, cost-based fee" for preparing the copy, provided the fee covers only labor associated with copying materials (whether the PHI was provided in paper or electronic form) and postage if the individual requested the copy be mailed. • The agency has removed a provision in the rules that gave covered entities 60 days to respond to requests for PHI when that PHI is stored offsite. All requests must be addressed (granted or denied) within 30 days, although covered entities are still permitted to grant themselves a one-time 30-day extension with notice given to the individual of the reasons for the delay.	• If PHI is maintained electronically in a designated record set, then it must be provided to the individual in the electronic form they request if that form is "readily producible." If PHI is not readily producible in the requested form, then the covered entity must agree with the individual on an alternate form and format in which to provide the copy of PHI. • Covered entities should consider the manner in which they would prefer to provide access to PHI on request from individuals. Although individuals are entitled to request PHI in any form they choose (within reason), for practical purposes individuals are likely to accept PHI in a readable format suggested by the covered entity and you should be ready to make that suggestion to avoid an unreasonable request by the individual. • HHS provides that covered entities are permitted to send individuals unencrypted emails including ePHI if the individual requests it, provided the covered entity has advised of the individual of the risk and the individual still prefers to receive the message by unencrypted email. The agency states that it does not expect covered entities to educate individuals about encryption technology and information security, but rather to notify the individual that there may be some level of risk that the information in the unencrypted email could be read by a third party. This statement by the agency is important to note because it does not strictly conform to the analysis prescribed by the Security Rule when a covered entity considers whether to use encryption. We advise that covered entities capture individuals' written acknowledgement of warnings the covered entity provides regarding unencrypted emails, or to contemporaneously document that the warning was given if done verbally. • HHS confirms in its preamble to the final rules that covered entities are not responsible for safeguarding information once delivered to the individual. • Covered entities should modify procedures to reflect that individuals must be provided with an electronic copy of PHI if requested, and that copies should be provided to a designated individual at the covered entity's request. Covered entities should develop forms that are designed to collect the necessary written, signed designation that is required in order to permit individuals to designate recipients of PHI.

"HHS provides that covered entities are permitted to send individuals unencrypted emails including ePHI if the individual requests it, provided the covered entity has advised the individual of the risk and the individual still prefers to receive the message by unencrypted email."

Restrictions on Disclosures to Health Plans Regarding Services Paid for Out-of-Pocket

Key Provisions	What the Provisions Mean for You
• The final rules provide individuals with the right to restrict certain disclosures of PHI to health plans. Specifically, if an individual requests it, a covered entity must restrict disclosures of PHI if: o The disclosure is to a health plan for purposes of carrying out payment or health care operations; o The disclosure is not otherwise required by law; and o The PHI pertains solely to a health care item or service for which the individual, or a party other than the health plan, has paid the provider in full.	• Unlike other individual requests for restricted disclosures, the final rules do not permit covered entities to unilaterally decline requests that meet this new standard imposed by the HITECH Act. A covered entity does have some discretion to decline an individual's request for this type of restriction, such as if the disclosure is for treatment purposes, if the individual did not pay in full for the health care item or service in question, if some or all of the payment was made by the health plan, or if the disclosure in question is not to a health plan. • Consistent with the proposed version of these rules, HHS states that individuals cannot expect out-of-pocket payments to count against their deductibles or similar thresholds if they request disclosure of PHI in this manner. Payments from FSA and HSAs are considered payments by the individual that might entitle them to requested restrictions of PHI, but the individual cannot expect the requested restriction to extend to the disclosure of PHI to the FSA or HSA since those disclosures may be necessary to secure payment. • HHS states that this right to request restrictions does not obligate providers to maintain separate medical records or otherwise segregate PHI. Rather, providers may flag certain PHI in a single medical file to denote the restriction. HHS opines that covered entities should be capable of such flagging due to their familiarity with and implementation of minimum necessary policies, which require limiting PHI disclosed to health plans to only that reasonably necessary to achieve the purpose of the disclosure. • HHS notes that when a provider is required by law to disclose PHI, it will not be obligated to honor an individual's request to restrict disclosures, such as where participation in a federal health plan like Medicare or Medicaid requires disclosure of the PHI in question. Similarly, where state law compels disclosure of PHI, the provider may comply with law and disregard an individual's requested disclosure. HHS notes, however, that these federal and state legal frameworks may also provide a means for individuals to request restrictions on disclosures, in which case the requested restriction must be honored. • HHS provides guidance in its preamble to these rules on situations in which an individual requests a restriction of PHI related to one of several encounters, or one of several services provided in a single encounter, generally noting its expectation that providers will accommodate and effectuate the individual's request and counsel them on the effect of the restriction. • HHS declined to require providers to notify all downstream providers (such as pharmacists) of the individual's request to restrict disclosures of PHI when a service is paid for out-of-pocket due to the lack of automated mechanisms to effectuate such downstreaming of the request and the high burden it would place on covered entities to do so.



Additional Permitted Uses and Disclosures of PHI

Key Provisions	What the Provisions Mean for You
• HHS has expanded slightly some of the permitted disclosures available under the Privacy Rule, providing that when an individual is not present a covered entity may disclose PHI to persons involved in the individual's health care, or payment for health care, if the PHI is relevant to the person's involvement. • In addition, regarding deceased individuals, covered entities may disclose PHI to family members or those involved in the individual's health care, or payment for health care, prior to the individual's death, provided the PHI is relevant to the person's involvement and provided the disclosure would not be inconsistent with any prior expressed preference by the individual that is known to the covered entity. • HHS has provided covered entities may disclose PHI to schools regarding individuals who are students or prospective students of the schools, if the PHI is limited to proof of immunization and the school is required by state or other law to have such proof of immunization prior to admitting the individual. Before so doing, the covered entity must obtain and document agreement to the disclosure from either: o A parent, guardian, or other person acting in *loco parentis* of the individual, if the individual is an unemancipated minor; or o The individual, if the individual is an adult or emancipated minor.	• Covered entities should revise applicable policies and training to account for these additional permitted disclosures of PHI. Note that these newly permitted disclosures are fairly limited in scope and are somewhat subjective in application. • Although HHS undoubtedly meant well in loosening the restrictions on disclosures to family members and others who cared for a decedent, the new provisions in this regard create a minefield for the unwary covered entity. Disclosures of PHI regarding decedents made to family members and other "involved" individuals must be limited to only PHI that is relevant to the nature of the recipient's involvement, a subjective standard. In addition, the disclosures must be consistent with any preference the decedent may have expressed to the contrary and that is known to the covered entity. If one family member claims to have been told by the decedent that another family member should not be made aware of certain PHI, will the covered entity be considered to "know" the decedent's wishes? But on the bright side the disclosure can be safely made 50 years later… In seriousness, it should be noted that these disclosures about decedents are permitted, not required, so in cases of doubt covered entities may prefer to err on the side of declining to disclose PHI. • The modifications described here are not intended to affect the rights of personal representatives to receive information about decedents or others. • Regarding disclosure of immunization records to schools, covered entities may rely on essentially any form of agreement (e.g., in person, by phone, via email) to the disclosure, but need to document that such agreement was obtained. Retaining a copy of a written request may suffice if the request makes clear the nature of the request (that it was made to obtain immunization records for a school). If the request was not received in writing, then a covered entity must document the request in order to rely on this new provision. HHS opines that a notation in the patient's medical records would suffice. The documentation regarding the request or agreement need not be a full-blown HIPAA authorization. • State law variations may affect disclosures of immunization records. For example, state law will dictate which schools are required to receive such records. HHS also notes that where state law mandates such disclosures to schools, the disclosure may be permitted by the Privacy Rule without regard to this new provision since the rule allows disclosures of PHI that are required by law. Where state law permits but does not require the disclosure, then this new HIPAA provision will imply and require written agreement by the appropriate party.

Modifications to Notice of Privacy Practices

Key Provisions	What the Provisions Mean for You
• Several of the rule changes implemented by HHS will necessitate corresponding changes to notices of privacy practices, such as inclusion of a description of uses and disclosures that require an authorization, which will include use or disclosure of PHI for marketing, selling PHI, and use or disclosure of psychotherapy notes (refer to sections regarding Marketing and Treatment Communications and Sale of PHI for additional information). • The notice must describe uses and disclosures of PHI for fundraising, and note the individual's right to opt out of such uses and disclosures (refer to section regarding Fundraising Communications for additional information); • For covered entities that are health plans and intend to use PHI for underwriting purposes, the notice must advise the individual that the covered entity is prohibited from using genetic information for underwriting purposes (refer to section regarding Genetics for additional information). • The notice must advise the individual of the covered entity's legal obligation to notify the individual if their PHI is affected by a security breach. • Notices made available by health care providers 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 section regarding Restrictions on Disclosures to Health Plans). • HHS has modified the method by which health plans are to notify participants of material changes to their notices of privacy practices. Health plans that post their notices on their websites may prominently post the change or its revised notice, and in its next annual mailing must provide the revised notice, or information about the material change and how to obtain the revised notice. Health plans that do not post their notice on their websites must provide the revised notice, or information about the material change and how to obtain the revised notice, to participants within 60 days of the revision. Health plans are still required to remind participants of the availability of the notice at least once every three years.	• The required modifications dictated by the final rules are very likely to require redrafting notices of privacy practices. HHS states that covered entities do not have to update notices if they already made changes to implement HITECH, provided the provisions of current notices are consistent with the final rules' requirements. However, several of the modifications described in these final rules are unlikely to have been anticipated and so may not have been taken into account in updated versions of notices. • Assuming the newly-required disclosures are not included in covered entities' current notices, the updates mandated by the final rules must be implemented. The modifications will constitute material changes, meaning that covered entities must promptly post or redistribute their notices before or on the compliance date. Providers should post the revised notice and health plans will be required to republish or recirculate their notices in one of the ways permitted by the final rules, described herein. • Although the notice must alert individuals of their right to opt out of fundraising communications, the notice need not describe the mechanism by which this right can be exercised. Rather, the opt-out mechanism is to be included or described in the fundraising communication (refer to section regarding Fundraising Communications for additional information.) • The agency acknowledges that covered entities may use layered notices (such as a short form notice supported by a full notice) if the notice delivery requirements of the final rules are otherwise fulfilled. • HHS has retained the requirement for individuals to opt in before they may receive notices electronically, such as via email, in lieu of the usual distribution requirements.

Compound Authorizations

Key Provisions	What the Provisions Mean for You
• Under the final rules, an authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study. • Despite this added flexibility, however, an authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes, and may not be combined with other authorizations.	• The research community has for the most part opposed HIPAA's general prohibition on combining authorizations, noting the administrative and documentation burdens and pointing out that requiring separate forms for related research activities is inconsistent with current practice under the Common Rule. Those who commented on HHS's proposed version of these rules also noted that multiple authorization forms may be confusing to research subjects, could dissuade individuals from participating in the study, and distract individuals from important content regarding potential use and disclosure of PHI since the use of separate authorizations necessitates repetitive language about the study across each form. • The final rules now expressly permit covered entities to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. • Covered entities affected by this modification may wish to revise their authorization forms or processes to take advantage of this change, taking care to highlight and distinguish the effect of an individuals' choice to opt in to conditioned or unconditioned research activities. It would also be useful to consider in advance how future revocations will operate, and to develop a means of soliciting from individuals revocations that are clear in terms of their scope and effect. In other words, where compound authorizations are used, it may be difficult to determine whether an individual revoking that authorization in the future intends to revoke it in whole or in part. Absent clarity on this point, the revocation would have to be deemed a complete revocation of the entire compound authorization. To avoid confusion on this point in the future, covered entities should consider what means they have available to establish clear, delineated revocation options from individuals if they prefer to only partially revoke compound authorizations.

"The final rules now expressly permit covered entities to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities."

Authorizations to Use and Disclose PHI for Future Research

Key Provisions	What the Provisions Mean for You
• Historically, HHS has interpreted the Privacy Rule to require that authorizations for research be study-specific due to the Privacy Rule's requirement that valid authorizations include a description of each purpose of use or disclosure of PHI. That interpretation appeared to rule out, or at least cast doubt on, the validity of authorizations in which the individual agreed to use and disclosure of PHI for potential future research, since future research could not be described in detail. • HHS has now stated in the preamble to these final rules that it is modifying its former interpretation of HIPAA's authorization requirements to provide that research authorizations need not be study specific where they pertain to future research.	• Authorization requirements otherwise remain the same (i.e., a specific description of current research activities is required and must be "study specific"), but a request to use PHI for future studies may be generalized and not study specific in recognition of the fact that it may not be possible to fully describe such studies in detail due to their prospective nature. • HHS provides that authorizations for future research "must adequately describe [future research] purposes such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research." The agency does not provide clear guidance on the types of statements that would satisfy its modified interpretation. Instead, HHS provides instead that a flexible interpretation that evolves over time will best harmonize with practices under the Common Rule, and seems to defer to covered entities, researchers and Institutional Review Boards in determining the types of statements that would adequately describe a future research purpose. Accordingly, individuals can authorize uses and disclosures of PHI for future research, but the adequacy of "future research purpose" authorizations appears to be left largely to covered entities, researchers and IRBs to determine in light of the circumstances of a particular study.

"Authorization requirements otherwise remain the same (i.e., a specific description of current research activities is required and must be 'study specific'), but a request to use PHI for future studies may be generalized and not study specific in recognition of the fact that it may not be possible to fully describe such studies in detail due to their prospective nature."

SECURITY REQUIREMENTS

Application of the Security Rule to Business Associates and Subcontractors

Key Provisions	What the Provisions Mean for You
• The Security Rule now applies in full to business associates (and their subcontractors). The Security Rule mandates a variety of comprehensive security measures, 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; 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; encryption; integrity controls; and appropriate written agreements with contractors. • Business associates are required to have appropriate agreements in place with subcontractors that access PHI, which include specific provisions mandated by the final rules.	• Covered entities should ensure that business associates comply with the Security Rule and other applicable portions of these rules that now apply directly to them. That increased vigilance is advisable not only because covered entities can be directly liable for business associate noncompliance, but also due to enhanced breach notification requirements (covered entities must report breaches caused by business associates unless they contract otherwise) and the agency's enhanced fining authority. Business associates should undertake Security Rule implementation now and redouble any existing efforts to comply prior to the September 23, 2013 compliance deadline (refer to the section regarding Business Associates for additional information). • Business associates will need to execute compliant business associate agreements with their subcontractors, and can expect to see their covered entity clients pushing out tougher business associate agreements that will seek liability protections such as indemnification.

"Business associates will need to execute compliant business associate agreements with their subcontractors, and can expect to see their covered entity clients pushing out tougher business associate agreements that will seek liability protections such as indemnification."

Scope and Application of the Security Rule to Covered Entities

Key Provisions	What the Provisions Mean for You
• The final rules retain the "flexibility of approach" measures that permit covered entities (and now business associates) to take into account their size and capabilities, the cost of the security measures, and the nature of the security risks they face when deciding which security measures to implement. • HHS has clarified that the Internet, extranets and intranets are forms of electronic media because they transmit data electronically. • HHS has clarified that certain transmissions of PHI (paper via fax and voice via phone) are not electronic media if they "did not exist in electronic form *immediately before* the transmission." • Photocopiers, fax machines and other office equipment that store ePHI, even if that was not intended by the user of the device, are considered electronic media covered by the Security Rule. • Genetic information is expressly included within the definition of "health information" and so will be subject to HIPAA rules if it is individually identifiable.	• On its face, not much has changed in the Security Rule for covered entities. However, HHS's enforcement actions and the results of its audits through 2012 have demonstrated that the agency's expectations on Security Rule compliance are generally not being met by covered entities. In light of increasing fines, ongoing audits, and the prospect of breach reporting, it's time to redouble your efforts to comply with this rule. • The retention of the "flexibility of approach" in the Security Rule means that security still will not be a "one size fits all" proposition for covered entities and business associates. Although that is good news, do not forget that the Security Rule always requires documentation to support your decision not to implement the security measures it mandates. If you choose an alternative measure, you have not complied with this rule until your decision is analyzed, justified, and documented using the factors the rule presents. • Applicable parts of the Security Rule will apply to transmissions of ePHI across the Internet, extranets and intranets – no surprise. The fact that you don't own the Internet or a particular website does not mean that you are free to send ePHI across them without concern for Security Rule compliance. And your intranet is not out-of-scope just because it is "all internal." That was the case before, but hopefully the agency's clarification will dispel these popular "HIPAA myths." • VOIP and electronic fax are not "electronic media" subject to the Security Rule if the fax started out in paper form and the phone discussion or voice message started out as an oral communication just before they were transformed into electronic communications. But the message that resulted and that sits in your Outlook application and on your email exchange server is in electronic storage and is covered by the Security Rule. • Individually identifiable genetic information in electronic form will be subject to Security Rule requirements (when handled by entities subject to HIPAA); that was a logical application of the rules prior to this modification, but now the agency has confirmed that HIPAA Rules apply to genetic information.

GENETIC INFORMATION

Genetic Information Nondiscrimination Act (GINA) Requirements

Key Provisions	What the Provisions Mean for You
• The final rules expressly include "genetic information" in the definition of "health information." Genetic information is defined as, with respect to an individual, information about: o The individual's genetic tests; o The genetic tests of the individual's family members; o The manifestation of a disease or disorder in the individual's family members; or o Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual. • All health plans covered by the Privacy Rule other than issuers of long-term care policies are prohibited from using or disclosing PHI that is also genetic information for underwriting purposes. • Although GINA does not define "manifested," HHS has decided to adopt a definition, which provides "a disease, disorder or pathological condition, that an individual has been or could reasonably be diagnosed with . . . by a health care professional with appropriate training and expertise in the field of medicine involved. . . . [A] disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information." • Other key terms are also defined in the final rules, such as "family member," "genetic tests," "genetic services," and "underwriting."	• HHS decided to apply GINA's prohibition on use of genetic information for underwriting purposes to all health plans subject to HIPAA, rather than the more limited set of plans covered by GINA. HHS was persuaded, however, to exclude issuers of long-term care policies from the prohibition, recognizing the impact such a prohibition would have on that particular insurance market. • Genetic information includes manifestations of a disease or disorder in the individual's family members. That's fancy talk for good old-fashioned family medical history. • GINA's prohibitions do not apply to conditions that have "manifested" in the individual. The agency posits that there is no bright line rule for determining whether a condition has manifested; this determination needs to be made on a case-by-case basis. For example, assume an individual has a family member that has been diagnosed with Huntington's disease and a test result indicates the presence of the Huntington's disease gene variant in the individual. Assume also that the individual is examined by a neurologist because he is experiencing occasional moodiness and disorientation (symptoms associated with Huntington's disease), but the results of the examination do not support a diagnosis of Huntington's disease. Huntington's would not likely be considered to have "manifested" under the meaning given in these final rules. The manifestation of the disease in a family member and/or the genetic test results are "genetic information" and cannot be used by a health plan for the purpose of underwriting. However, if the individual exhibited further symptoms such that Huntington's could reasonably be diagnosed by the neurologist, then the health plan would be able to account for the disease for underwriting purposes, provided the diagnosis was not based primarily on the test results or other "genetic information," but rather was based primarily on the "manifestation" of the disease in the individual. • A health plan may consider the manifestation of a disease or disorder in a family member when the family member is the subject of the underwriting determination. For example, if an individual enrolls in a health plan that will also cover her immediate family, the health plan may consider the manifested conditions of the family members who are to be covered by the plan. The health plan may not, however, use manifested conditions of one covered family member as genetic information about another family member to further inform underwriting. • A health plan may receive, use and disclose "genetic information" to determine the medical appropriateness of an individual benefit. These rules also do not prohibit a plan from receiving genetic information during claims payment. Rather, the prohibitions pertain specifically to use of genetic information for underwriting. • Health plans may need to revise and distribute their notice of privacy practices as a result of these modifications. (Refer to section on Notice of Privacy Practices for additional information.)

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

ELIZABETH JOHNSON leads Poyner Spruill's Privacy and Information Security Practice Group. 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, academia, 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 is consistently listed among the "Legal Elite" in North Carolina by Business North Carolina and recognized as a North Carolina "Super Lawyer" by the publishers of Law and Politics Magazine.

Elizabeth is a frequent speaker and lecturer on information security and privacy topics. She earned a JD and a Master's degree at Duke University, and a BA from Coe College. She can be reached at 919.783.2971, or ejohnson@poynerspruill.com and you may follow her on Twitter @PoynerPrivacy.

301 Fayetteville St., Suite 1900, Raleigh, NC 27601