A Dialogue on HIPAA/HITECH Compliance: Considerations Now That the HITECH Rules are Here

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.

Conflict of Interest Disclosure

Leon Rodriguez, JD

James B. Wieland

Have no real or apparent conflicts of interest to report.

Learning Objectives

1. Provide insights on the real-world applications of the new privacy and security rules
2. Discuss the practical implications of the final breach notifications rule
3. Provide an update on future OCR directions and priorities for investigations, enforcement and audits

Omnibus Final Rule – Important Dates

- Public Display at Federal Register – January 17, 2013
- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Conform BA contracts – September 22, 2014

Omnibus Final Rule – What's New for Consumers

- Right to Electronic Copy of Electronic Health Record
  - Right to direct copy to designated 3d party
- Prohibition on Sale of PHI without Authorization
- Marketing Communications Paid for by 3d Party Require Authorization
  - Limited exceptions for refill reminders and current prescriptions
- Easy Way to Stop Fundraising Communications
- Right to Restrict Disclosures to Health Plans of Treatment/Services Paid for Out of Pocket

GINA Provisions

- Requires “Genetic Information” to be treated as PHI
- Prohibits Health Plans from using/disclosing genetic information for underwriting purposes
- Terms and definitions track regulations prohibiting discrimination in provision of health insurance based on genetic information

Omnibus Final Rule – Non-statutory Provisions

- Student Immunization
  - Makes it easier for parents to permit providers to release student immunization records to schools
- Research
  - Allows researchers to use single authorization for more than one research purpose
  - Relaxes policy on authorizations for future research
- Notice of Privacy Practices
  - Updates required to Notices of Privacy Practices
  - Relaxes distribution requirements for Health Plans
- Decedent Information
  - Protections limited to 50 years after death
  - Eases access to friends and families

Omnibus Final Rule – What's New for Business Associates

- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule
  - Liable for Security Rule violations
- BA must comply with use or disclosure limitations expressed in its contract and those in the Privacy Rule
  - Criminal and civil liabilities for violations
- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities
- Subcontractors of a BA are now defined as a BA
  - BA liability flows to all subcontractors

Omnibus Final Rule – What's New for Breach

- Breach Notification Provisions
  - Replaces "harm to individual" with more objective measure of compromise to the data as threshold for breach notification
  - Other provisions of 2009 IFR adopted without major change

Breach Notification Highlights

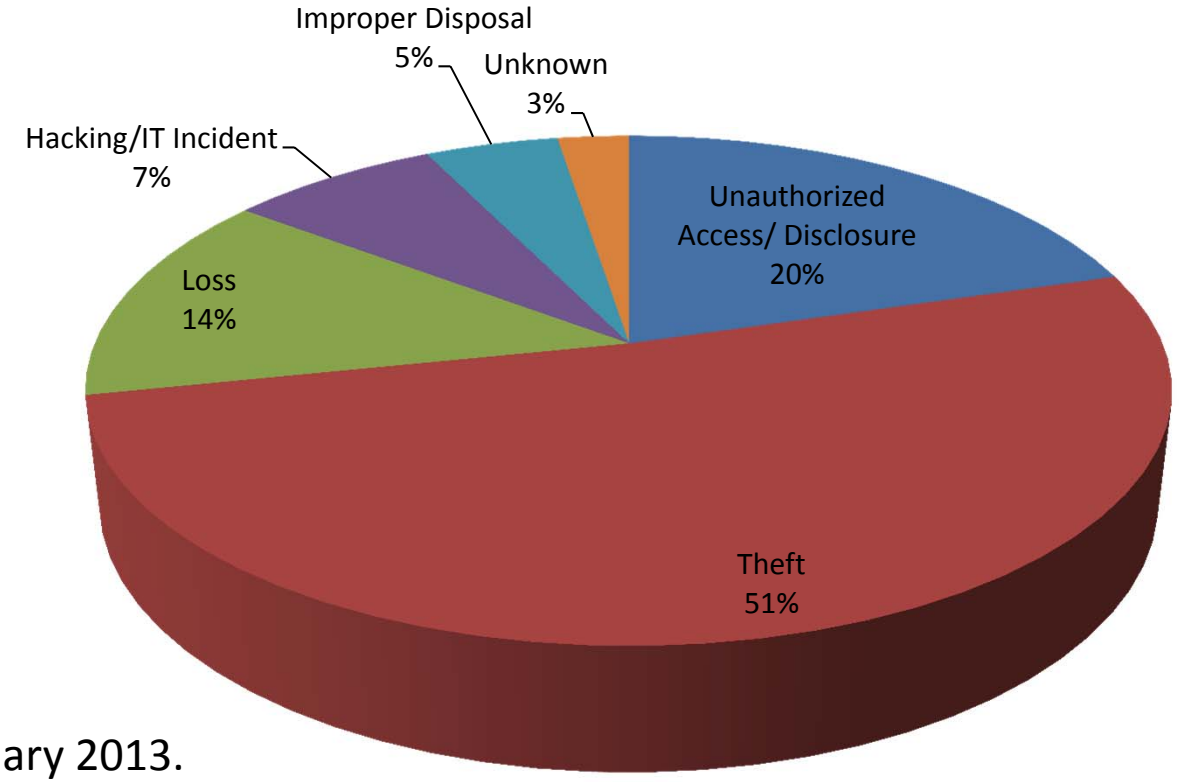
September 2009 through February 20, 2013

- 543 reports involving over 500 individuals
- Over 64,000 reports involving under 500 individuals
- Top types of large breaches
  - Theft
  - Unauthorized Access/Disclosure
  - Loss
- Top locations for large breaches
  - Laptops
  - Paper records
  - Desktop Computers
  - Portable Electronic Device

Spotlight on Largest Breaches of 2012

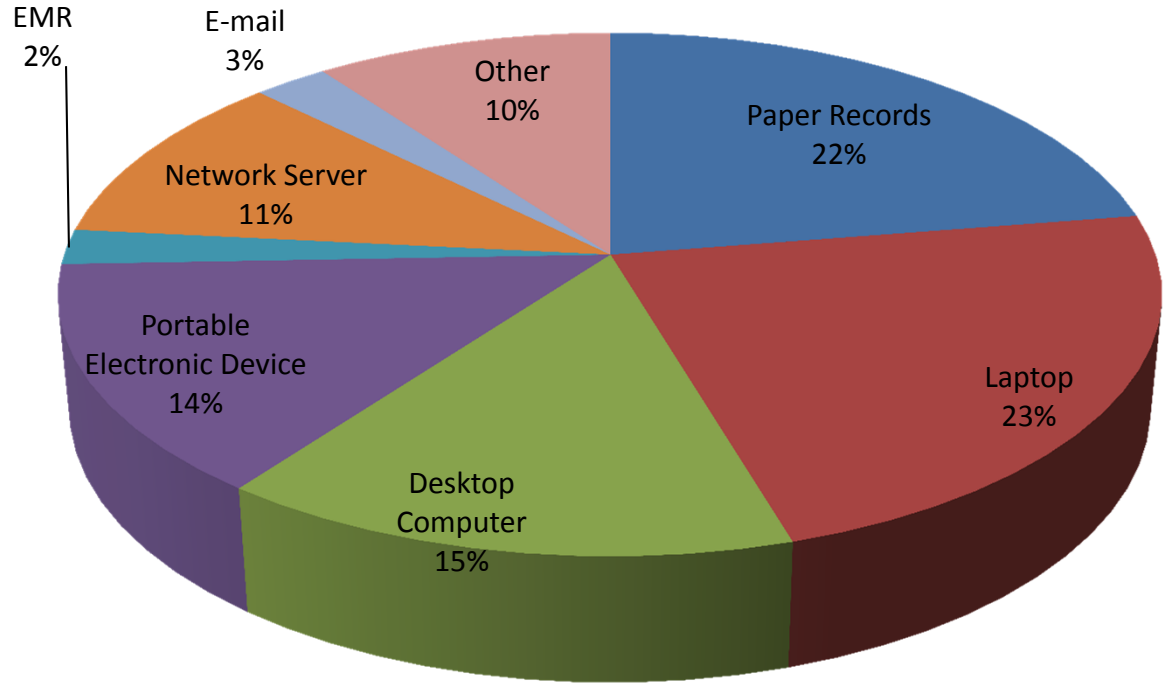
- Hacking network server – 780,000 affected
- Backup tapes stored at hospital cannot be found and are presumed lost– 315,000 affected
- Unencrypted emails sent to employee's unsecured email address -- 228,435 affected
- Theft of laptop from employee's vehicle– 116,506 affected
- Unauthorized access to e-PHI stored in database-- 105,646 affected
- Hacking database stored on network server – 70,000 affected

Breach Notification: 500+ Breaches by Type of Breach



Data as of January 2013.

Breach Notification: 500+ Breaches by Location of Breach



Data as of January 2013.

Omnibus Final Rule – What's New for Enforcement

- Enforcement Provisions
  - Adopts increased CMP amounts and tiered levels of culpability from 2009 IFR
  - Clarifies "Reasonable Cause" Tier
  - Willful Neglect Penalties do not require informal resolution
  - Intentional wrongful disclosures may be subject to civil, rather than criminal, penalties

HITECH Enforcement Raises CMP Levels

Violation Category	Each Violation	All Identical Violations per Calendar Year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect-Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect-Not Corrected	$50,000	$1,500,000

HIPAA Compliance / Enforcement
(As of December 31, 2012)

TOTAL (since 2003)	
Complaints Filed	77,200
Cases Investigated	27,500
Cases with Corrective Action	18,600
Civil Monetary Penalties & Resolution Agreements (since 2008)	$14.9 million

Major 2012 Enforcement Actions

- BCBS Tennessee ($1.5 M)
  - E-PHI stored on servers stolen from deactivated data center after construction/relocation to new facility
  - Reevaluate threats/vulnerabilities to e-PHI caused by changing operational environment and manage risk
- Phoenix Cardiac Surgery ($100K)
  - E-PHI disclosed through Internet when provider used third party application hosted in the cloud
  - Business associate agreements required when sharing data with cloud computing service providers
- Alaska DHSS ($1.7M)
  - Portable storage device stolen from personal vehicle symptomatic of widespread failure to implement program-wide information security safeguards
  - Risk analysis to identify location and safeguards for PHI, training and controls for portal devices

U.S. Department of Health and Human Services, Office for Civil Rights

Major Enforcement Actions of 2012

- Massachusetts Eye and Ear Institute ($1.5M)
  - Stolen personal laptop of physician using device as desktop substitute
  - Covered entity had not implemented a program to mitigate identified risks to e-PHI
  - Encrypt data stored on end-user devices
- Hospice of Northern Idaho ($50K)
  - Breach affecting 400 individuals when laptop stolen
  - Provider had not conducted a risk assessment or taken other measures to safeguard e-PHI as required by Security Rule
  - Implement security measures to safeguard e-PHI

Audit Program

- HITECH Act – Sec. 13411
  - Periodic audits to ensure covered entities and business associates comply with requirements of HIPAA and HITECH

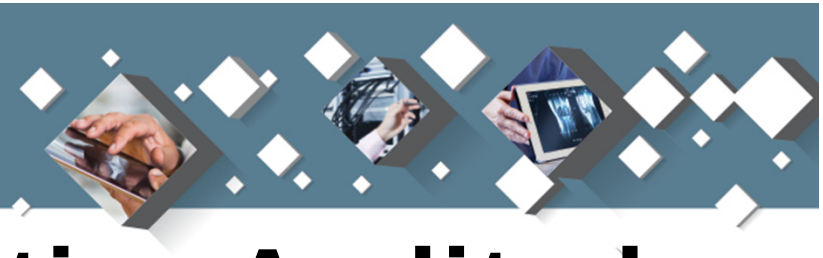
- Audit Objectives
  - Examine mechanisms for compliance
  - Identify best practices
  - Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
  - Renew attention of covered entities to health information privacy and security compliance activities

Audit Pilot Completed

- Pilot Process
  - Tiered approach for snapshot of compliance across covered entity types, sizes, complexity
  - Sample of 115 covered entities selected spread across 4 tiers
  - All audits completed by December 2012
  - Published audit protocol
  - Issuing final reports to 115 entities audited in pilot and assessing findings
- Conducting Evaluation of Audit Pilot

Audit Pilot Observations

- Completed Audits of 115 entities
  - –61 Providers, 47 Health Plans, 7 Clearinghouses
- No findings or observations for 13 entities (11%)
  - –2 Providers, 9 Health Plans, 2 Clearinghouses
- Total 979 audit findings and observations
  - – 293 Privacy
  - – 592 Security
  - – 94 Breach Notification
- Percentage of Security Rule findings and observations was double what would have been expected based on protocol
- Smaller entities (*Level 4)* struggle with all three areas



Size / Type of Entities Audited

	Level 1	Level 2	Level 3	Level 4	Total
Health Plans	13	12	11	11	47
Healthcare Providers	11	16	10	24	61
Healthcare Clearinghouses	2	3	1	1	7
Total	26	31	22	36	115

Data as of December 2012.

Level 1 Entities

- Large Provider / Payer
- Extensive use of HIT - complicated HIT enabled clinical /business work streams
- Revenues and or assets greater than $1 billion

Level 2 Entities

- Large regional hospital system (3-10 hospitals/region) / Regional Insurance Company
- Paper and HIT enabled work flows
- Revenues and or assets between $300 million and $1 billion

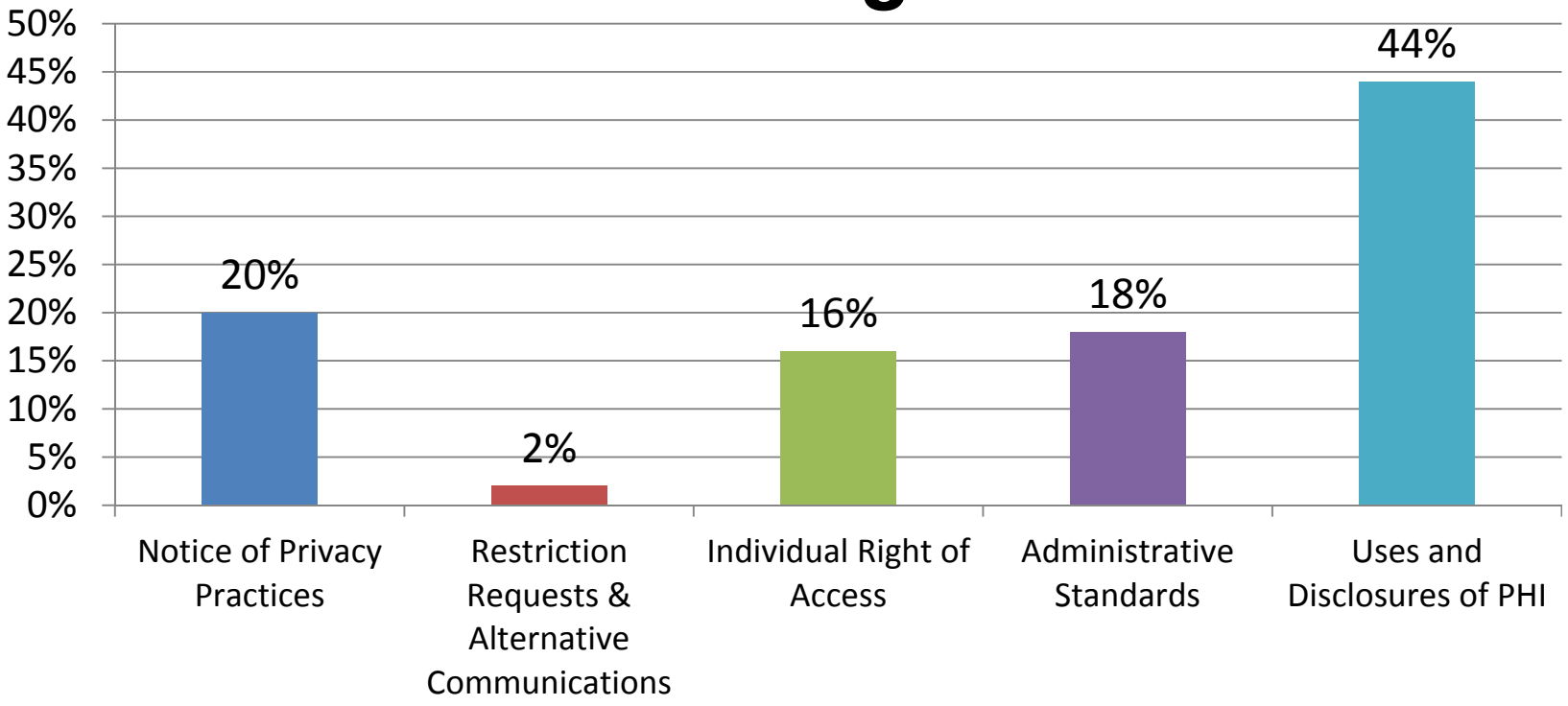
Level 3 Entities

- Community hospitals, outpatient surgery, regional pharmacy / All Self-Insured entities that don't adjudicate their claims
- Some but not extensive use of HIT – mostly paper based workflows
- Revenues between $50 million and $300 million

Level 4 Entities

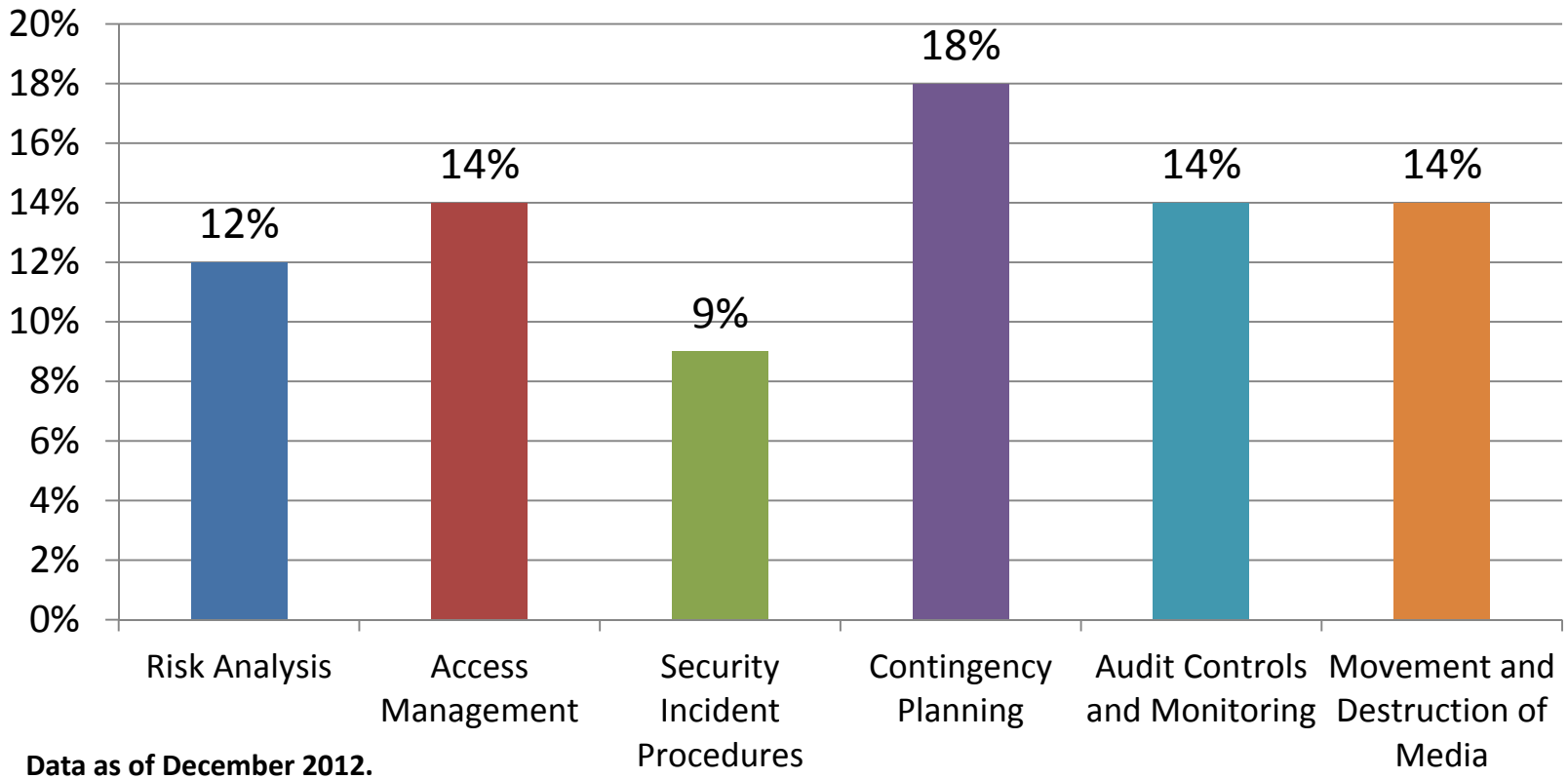
- Small Providers (10 to 50 Provider Practices, Community or rural pharmacy)
- Little to no use of HIT – almost exclusively paper based workflows
- Revenues less than $50 million

Types of Privacy Rule Audit Findings



Data as of December 2012.

Types of Security Rule Audit Findings



Data as of December 2012.

Medscape: Free CME and CE Training

HIPAA: Creating Awareness and Educating Providers on the Importance of Compliance

Credits Available

Physicians - maximum of 0.50 *AMA PRA Category 1 Credit(s)™*

You Are Eligible For

- AMA PRA Category 1 Credit(s)™

Accreditation Statements

For Physicians

Medscape

Medscape, LLC is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

http://www.medscape.org/viewarticle/762170?src=cmsocr

ONC/OCR Mobile Device Program Instructional Video Series

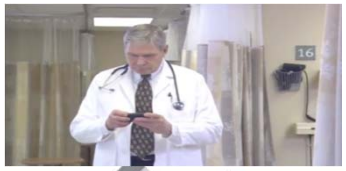
The videos explore mobile device risks and discuss privacy and security safeguards providers and professionals can put into place to mitigate risks.

Securing Your Mobile Device is Important!

Dr. Anderson's Office Identifies a Risk

A Mobile Device is Stolen

Can You Protect Patients' Health Information When Using a Public Wi-Fi Network?



Worried About Using a Mobile Device for Work? Here's What To Do!

Downloadable Materials

www.healthit.gov/mobiledevices

- Fact sheets
- Posters
- Brochures

Mobile Device Program: Tips to Protect and Secure Health Information

Use a password or other user authentication.

Install and enable encryption.

Install and activate wiping and/or remote disabling.

Disable and do not install file- sharing applications.

Install and enable a firewall.

Install and enable security software.

Keep security software up to date.

Research mobile apps before downloading.

Maintain physical control of your mobile device.

Use adequate security to send or receive PHI over public Wi-Fi networks.

Delete all stored health information before discarding or reusing the mobile device.

Questions?

OCR website www.HHS.gov/OCR

NEW ORLEANS
HIMSS13
ANNUAL CONFERENCE & EXHIBITION

HIPAA-HITECH and GINA Final Rule

March 4, 2013

James B. Wieland
jbwieland@ober.com

OBER | KALER
Attorneys at Law

Compliance Dates

On January 25, 2013, the Department of Health and Human Services (HHS) posted Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules (the Final Rule) under the authority of the HITECH Act and the Genetic Information Nondiscrimination Act (GINA).

- The Final Rule will be effective on March 26, 2013.
- However, in general covered entities and business associates will have an additional six months, until September 23, 2013, to come into compliance.
- The Final Rule does not address the Proposed Rule on Accounting for Disclosures, published May 31, 2011.
- The Enforcement Rule changes are effective on March 26, 2013. The additional 180 days afforded for most of the provisions in the Final Rule apply only to modified standards or implementation specifications.

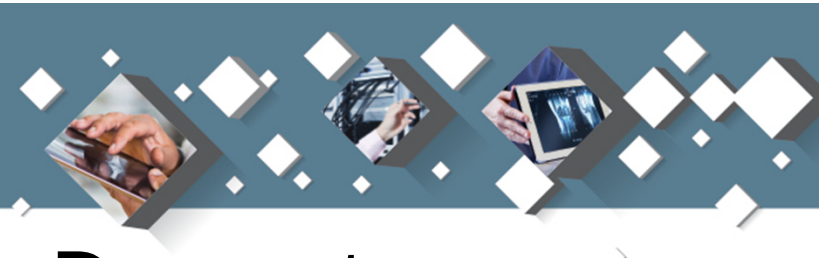
Business Associates: Conduits

In addition to formalizing the inclusion of Patient Safety Organizations and Health Information Organizations (Health Information Exchanges, E-Prescribing Organizations and similar organizations) as business associates, the Final Rule provides important clarification about the status of “conduits” as business associates.

- Since the inception of HIPAA, service providers such as the post office and telephone companies have been exempt from the business associate requirements as their access to Protected Health Information (PHI), if any, has been on an incidental, as opposed to a routine, basis.

Business Associates: Conduits

- As technology has evolved, the application of this test, never a “bright line,” to important health care industry service providers such as cloud service providers of storage or software, has been unclear.
- The Final Rule articulates a brighter line test. A conduit, whether of paper or electronic PHI, only provides transmission services, including any temporary storage of PHI incidental to the transmission service. By contrast, a service provider that provides storage is a business associate, even if the agreement with the covered entity does not contemplate any access or access only on a random or incidental basis. The test is persistence of custody, not the degree (if any) of access.



Business Associates: Downstream Contractors

- Downstream entities that work at the direction of or on behalf of a business associate and handle protected health information are required to comply with the applicable Privacy and Security Rule provisions, just like the "primary" business associate and are subject to the same liability for failure to do so.
- This specifically does not require the covered entity to have a contract with the subcontractor; rather, that obligation remains on each business associate.
- A "subcontractor" is an entity to which a business associate delegates a function, activity, or service involving covered entity's PHI, other than in the capacity of a member of the workforce of such business associate".
- A hospital contracts with a billing company. The billing company contracts with a shredding company to dispose of its billing records. The shredding company contracts with a trucking company to bring the hospital's paper billing records to its shredding facility.

Business Associates: Downstream Contractors

- Under the Final Rule, each entity would be directly responsible for compliance with the business associate requirements under the Security Rule and the Privacy Rule, even if the parties fail to enter into a written business associate agreement. The trucking company's responsibility would likely be based on custody, even if it did not view the records, as discussed above. Under the Final Rule, the hospital would only be required to enter into a business associate agreement with the billing company. The business associate or downstream subcontractor would be required to obtain written "satisfactory assurances" from its immediate subcontractor.
- In the event of a breach of the security of unsecure PHI, the chain of reporting would follow the chain of contracting in reverse: trucking company to shredding company; shredding company to billing company; billing company to hospital.

Business Associates: Privacy Rule Obligations

The Final Rule specifies the Privacy Act obligations of a Business Associate, not addressed in detail in the HITECH Act.

- Limiting uses and disclosures to what is permitted under the Privacy Rule, subject to what is allowed under the Business Associate Agreement. This specifically includes compliance with the minimum necessary standards;
- Providing breach notification to the covered entity;
- Providing a copy of electronic PHI to either the covered entity, the individual or to the individual's personal representative, as specified in the business associate agreement;
- For disclosing PHI to the Secretary in an investigation of the Business Associate's compliance with HIPAA;
- For providing an accounting of disclosures;
- For complying with the security rule.

Business Associates: Privacy Rule Obligations

Comments by the Secretary indicate that permitted disclosures by a business associate for its own management and administration or for legal purposes do not create a business associate relationship with the recipient because “such disclosures are made outside the entity’s role as a business associate.”

In that case, however, unless the disclosure is required by law, the business associate must obtain satisfactory assurances that the recipient will hold the information as confidential, will use or disclose it only for its intended purpose or as required by law, and will report a breach of confidentiality to the business associate.”

Business Associates: Transition Provisions

In recognition of the time that will be necessary to renegotiate existing business associate agreements, the Final Rule grandfathers certain business associate agreements for up to one year beyond the compliance date, up to September 23, 2014.

- In order to qualify, the business associate agreement must have been in existence prior to the publication of the Final Rule (January 25, 2013), have complied with HIPAA prior to the publication date and not be renewed or modified during the grandfather period.
- An automatic renewal, under a so-called evergreen clause, does not constitute a renewal or modification for purposes of the availability of the grandfather period.

Enforcement Rule: Investigation and Resolution of Violations

The Final Rule reflects the requirement of the HITECH Act that HHS will investigate a possible HIPAA violation if, as HHS states, a preliminary review of the facts available from a complaint or a compliance review, or information from an independent inquiry by HHS, indicates the possibility of willful neglect as to HIPAA compliance.

- The investigation may proceed directly to an enforcement action, particularly but not only, in the case of willful neglect.
- However, the Final Rule offers reassurance that, absent indications of willful neglect, HHS still will seek compliance through informal, voluntary action in appropriate cases.

Enforcement Rule: Violations Due to Reasonable Cause

Of the four tiers of penalties specified in the HITECH Act, the required state of mind for the "lowest" tier (entity did not know, and in the exercise of reasonable diligence would not have known of the violation) and for the "highest" two tiers (willful neglect) are unchanged under the Final Rule.

- The state of mind for second tier, violations due to reasonable cause not amounting to willful neglect, was not specified in the HITECH Act.

Enforcement Rule: Violations Due to Reasonable Cause

- The second tier is important as a practical matter, because it likely covers many common violations by otherwise generally compliant covered entities and business associates, such as those that occur due to human error, despite workforce training and appropriate policies and procedures.

- The Final Rule modifies the definition of reasonable cause to specify the state of mind; reasonable cause covers violations in which the entity exercised ordinary business care and prudence to comply with the provision that was violated or in which the entity knew of the violation but lacked "conscious intent or reckless indifference" associated with a violation due to willful neglect.

Enforcement Rule: Upstream Vicarious Liability

Under the Final Rule, compliance obligations flow downstream between parties with direct contractual relationships: Covered Entity to Business Associate, Business Associate to Subcontractor, and so on.

- If a business associate or downstream contractor is an agent of the entity with which it contracted under federal common law, civil monetary penalties imposed on the downstream contractor for a HIPAA violation will be attributable to the upstream party with which it contracted, so long as the underlying conduct was within the scope of the agency,.
- The Final Rule summarizes HHS's view of federal common law of agency. Determinations will be based on the right or authority of the upstream entity to control the downstream entity's conduct in the course of performing the service, even if that right was not actually exercised with respect to the violation for which the CMP is imposed.

Marketing

In a significant departure from the Proposed Rule, an authorization for treatment communications and for communications previously permitted without an authorization under health care operations is required ***if*** the covered entity or business associate receives financial remuneration from the third party whose product or service is subject to the communication.

- **Financial remuneration consists of direct or indirect payment from, or on behalf of, the third party whose product is the subject of the communication.**
- **An exception, in accordance with the HITECH Act, is made for subsidized refill reminders or communications about a currently prescribed drug or biological, as long as the subsidy is reasonable in amount.**
- **Direct means the payment is paid directly to the entity and indirect means that it was channeled through a third party.**
- **Financial *remuneration* does not include "in-kind" or other nonfinancial subsidies for this purpose (contrast with p*ayment* for the sale of PHI, discussed later).**

Marketing

The Proposed Rule required notice and an opt-out for subsidized treatment communications (defined as those sent to an individual) and an authorization for subsidized health care operations communications (defined as those sent to a population of individuals) about treatment or treatment alternatives, health-related products or services available from the covered entity, participants in or benefits available in a provider or health plan network (i.e., the exceptions to the definition of marketing in the definition of *health care operations*) was impractical to implement. This required a judgment as to whether a communication pertained to treatment or health care operations and required two separate processes for subsidized communications.

- In the absence of direct or indirect remuneration, no authorization is required for either the treatment or the health care operations communications. In addition, the exception for face-to-face communications or gifts of nominal value continues, without reference to remuneration from a third party.

Sale of PHI

The HITECH Act required an authorization if a covered entity or business associate received direct or indirect remuneration in exchange for the disclosure of PHI, a so-called “sale”.

- **Exceptions were specified in the Act for public health activities, research, treatment, the sale or other business consolidation of a covered entity, business associate services requested by the covered entity, fees charges for providing an individual with access to the individual’s PHI, and other purposes designated by HHS.**
- **The Final Rule defines sale of *PHI* as “a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.”**
- **Disclosure includes granting access directly or through licenses or lease agreements, not just transfers of title.**
- **Remuneration, for this purpose, includes non-financial, in-kind value.**

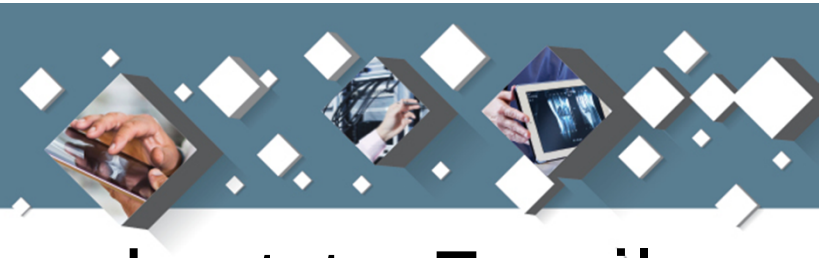
Sale of PHI

- As to disclosures to a business associate, the Final Rule makes it clear that a business associate may recoup reasonable cost-based fees from third parties for preparing or transmitting records on behalf of the covered entity or where otherwise permitted by law, and that remuneration paid by the business associate to a subcontractor for activities performed on behalf of the business associate does not require an authorization.

Research

The Final Rule permits covered entities to combine conditional and unconditional authorizations for research if they differentiate between the two activities and allow for an opt-in of unconditional research activities.

- Future research studies may now be part of a properly executed authorization, which includes all the required core elements of an authorization. Under the prior rule, covered entities could not combine or condition authorizations for purposes other than research that involves treatment, while a separate authorization was needed for future research or to create or build a central research database or repository.
- This change brings HIPAA in line with Common Rule requirements related to biospecimens and databases.
- The only exception applies to authorizations related to psychotherapy notes, which may be combined only with another authorization for the use or disclosure of psychotherapy notes.



Disclosures about a Decedent to Family Members and Others Involved in Care

Peviously, a covered entity could disclose information about a decedent only to a personal representative.

- Under the Final Rule, a covered entity also is permitted to disclose a decedent's information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless inconsistent with any prior expressed reference of the individual that is known to the covered entity.
- This change does not change the authority of a decedent's personal representative.
- The PHI of individuals deceased for fifty years or more is not protected under HIPAA.

Disclosures of Student Immunization to Schools

Under the Final Rule, covered entities may send immunization records directly to a school without written authorization. Instead, a covered entity may provide immunization records to a school upon the assent by a parent, guardian or person acting in loco parentis.

- These disclosures must comply with state law regarding the provision of immunization records. Covered entities must document their discussions related to disclosure for student immunization records.

Fundraising

The Privacy Rule permitted a covered entity to use or disclosure PHI to a business associate or related foundation for fundraising purposes without an individual's authorization. Permitted PHI included:

- Demographic information related to an individual
- Dates of health care provided to an individual.

Fundraising

The Final Rule clarifies what constitutes demographic information. It does not modify what constitutes fundraising communication and current opt out requirements, however.

- Under the Final Rule, covered entities are provided flexibility to decide the method to allow for individuals to opt out and opt back into the use of PHI in fundraising activities. For example, a covered entity could use a toll-free number, email address, other opt-out mechanism or a combination of methods.
- In addition, under the Final Rule HHS leaves the decision as to the scope of the opt-out related to future fundraising communications to the covered entity.
- Many covered entities found campaign-specific opt-outs difficult to track for compliance purposes. HHS strengthened the standard related to further communications after individuals opt out from reasonable efforts to an outright prohibition.

Notice of Privacy Practices

- Covered entities that did not modify their Notice of Privacy Practice after the passage of HITECH are now required to make changes and to make the new Notices available based on changes required under the Final Rule.
- For example, the Final Rule requires that a covered entity include uses and disclosures of PHI, but not specify a list of all situations in which an authorization is required. Instead, covered entities can list categories that require authorization, such as:
  - psychotherapy notes (if applicable)
  - marketing purposes
  - sale of PHI

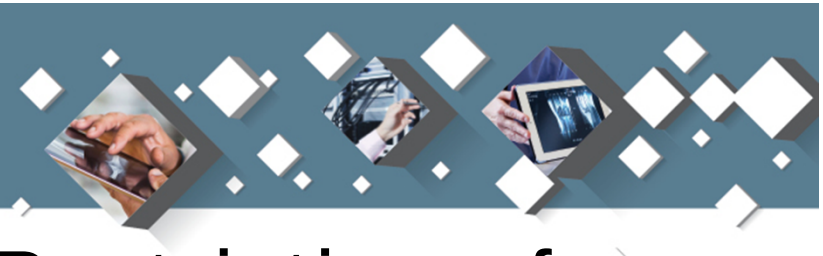
Notice of Privacy Practices

The Final rule adopts the provision obligating health plans that perform underwriting to include in their Notice of Privacy Practices a statement that the health plan is prohibited from using or disclosing genetic information for underwriting purposes. This change does not apply to issuers of long-term-care policies who for now, are exempted from the underwriting prohibition.

Notice of Privacy Practices

The Notice must also include a statement that other uses and disclosure not described in the Notice of Privacy Practices will be made only with authorization from the individual.

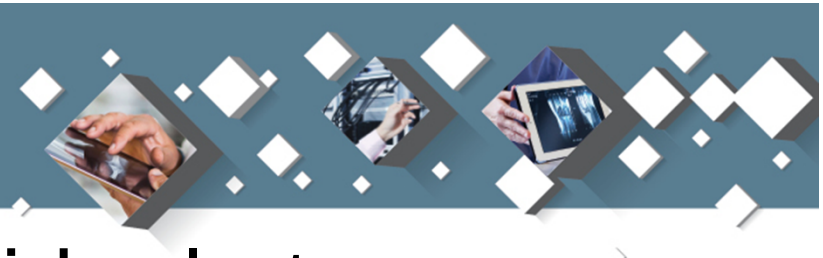
- The Notice of Privacy Practices must also include a statement related to fundraising communications and the individual's right to opt out, and the new right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service.
- Finally, the Notice of Privacy Practice must include a statement related to a breach of unsecured PHI, although an entity-specific statement is not required.



Right to Request a Restriction of Uses and Disclosures

The Final Rule creates a new right to restrict certain disclosures of PHI to a health plan where the individual or a family member or other person pays out of pocket in full for the health care item or service.

- Covered entities will be required to develop methods to create notation in an individual's medical record related to restrictions so that information is not sent to or accessible to health plans.
- Covered entities still can submit restricted information for required Medicare and Medicaid audits under the "required by law" requirement of the Privacy Rule.



Access of Individuals to Protected Health Info: Access

The Final Rule amends the Privacy Rule to allow individuals to request electronic copies of their PHI that is maintained in an electronic health record (EHR) or other electronic designated record set.

- Covered entities must provide an electronic, “machine readable copy,” which means digital information stored in a standard format enabling the PHI to be processed and analyzed by a computer.
- HHS provides flexibility as to the exact format, acknowledging that systems may vary, but requires the covered entity to accommodate individual requests for specific formats, if possible.

Access of Individuals to Protected Health Info: Third Party

Under the Final Rule, if an individual requests a covered entity send PHI directly to another individual, the covered entity must transmit the copy as requested. This request must:

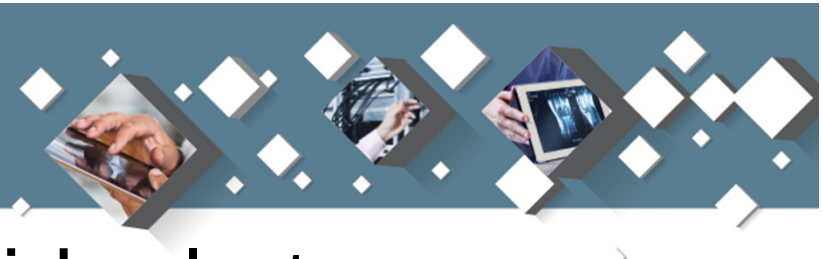
- be in writing and signed by the individual, and
- clearly identify the designated person and where to send the copy of the PHI.

If a covered entity already requires that access request be in writing, the covered entity can use the same request to access the individual's PHI or require a separate written request. Covered entities will need to implement policies and procedures to verify the identity of the person who requests PHI and safeguards to protect the information that is used or disclosed.

Access of Individuals to Protected Health Info: Fees

Under the Privacy Rule, Covered Entities can charge reasonable cost-based fees.

- The Final Rule allows the labor cost for copying PHI to be separately identified in both paper and electronic form as a factor in cost-based fees. HHS acknowledged that the labor cost for search and retrieval of PHI in electronic form are more than negligible.
- Covered Entities may also include the supply cost for both paper and electronic copies, including CDs or UBS flash drives, along with postage for sending portable media at the request of the individual.
- Fees related to maintaining systems, infrastructure and storage are not considered reasonable, cost-based fees. Covered entities should check state law related to fee restrictions and requirements.



Access of Individuals to Protected Health Info: Timeliness

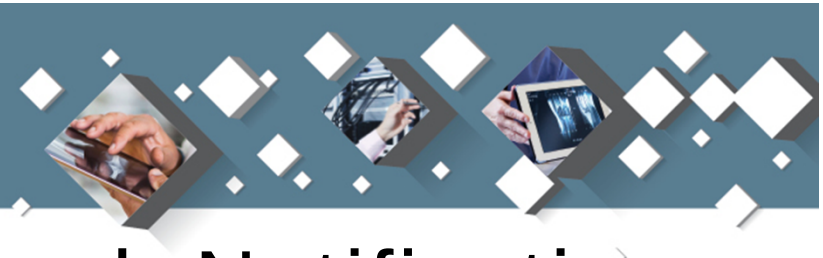
The Final Rule removes the 60-day timeframe for retrieval of records held off site, leaving covered entities with 30 days to provide access to records to individuals in all circumstance with a one-time 30-day extension.

- This change was made due to the increase reliance on electronic records and to encourage covered entities to provide access to records sooner.
- State law related to more stringent timeliness requirements should be reviewed.

Modifications to the Breach Notification Rule

The Interim Final Breach Notification Rule (the Breach Rule), published August 24, 2009, has been finalized mostly without change with one significant exception – the definition of a *breach* was "clarified" through the removal of the "harm threshold" , replacing it with a more objective test of whether PHI has been "compromised."

- Following the clarification, it is likely that more breaches will need to be disclosed and reported.
- These changes are characterized as a "clarification.
- Covered Entities and Business Associates should analyze breaches prior to the compliance date accordingly.



Modification to the Breach Notification Rule: Definition of Breach

Of the 85 public comments received on the definition of *breach*, 70 addressed the harm threshold. Of those 70 comments, 60 supported the existing standard, but 10 (from members of Congress and consumer advocacy organizations) argued for its modification or elimination.

The Secretary explained that it believes that the "language [defining *breach* and explaining the harm standard] used in the Interim Final Rule and its preamble could be construed and implemented in manners we had not intended."

As a result, in the Final Rule, the Secretary clarifies the "position that breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information is compromised."

Modification to the Breach Notification Rule: Definition of Breach

(including the harm standard)

This clarification was undertaken in two steps:

- First, language was added to the definition of a *breach* to "clarify that an impermissible use or disclosure of protected health information is presumed to be a breach" unless the responsible entity can demonstrate that "there is a low probability that the protected health information has been compromised."
- Second, the harm standard was removed and modifications were made to the risk assessment portion of the Breach Rule to require the use of a more objective risk assessment.

Modification to the Breach Notification Rule: Definition of Breach

The new standard is as follows:

- **Except as provided in [the existing exceptions to the definition of breach], an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that here is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:**
  - **(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;**
  - **(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;**
  - **(iii) Whether the protected health information was actually acquired or viewed; and**
  - **(iv) The extent to which the risk to the protected health information has been mitigated.**

Modification to the Breach Notification Rule: Definition of Breach

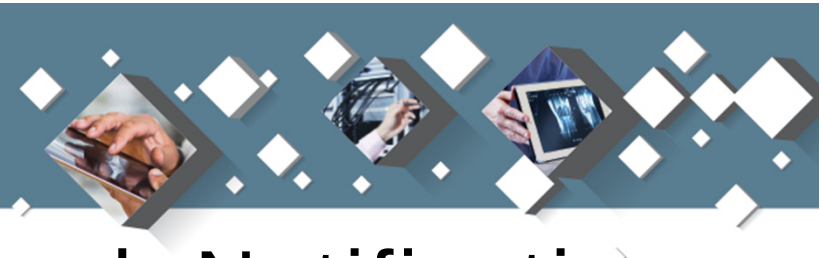
(including the harm standard)

The Final Rule also eliminates the existing regulatory exception for limited data sets that do not contain any dates of birth or zip codes. In the event of a breach including a limited data set, whether the data set contains dates of birth or zip codes is immaterial (though the type of information disclosed may play a role in the new assessment.

Modification to the Breach Notification Rule: Notification to Individuals

The Final Rule retains the Interim Final Rule's requirements for breach notifications without modification, but, provides some clarification on some of the finer points of when a breach is "discovered," the timeliness of notification, methods of notification, the content of the notice, and other sub-topics. Important clarifications include:

- The Final Rule noted that a covered entity that is *acting as a business associate* (by, for instance, providing billing or other services to another covered entity) should respond to a breach as a business associate. In these situations, the obligation to disclose will rest with the covered entity whose PHI is compromised.
- The Final Rule clarified several points regarding alternative notice and made explicit that notice *has not been given* if a written notice is returned as undeliverable. Covered entities responding to a breach with more than 10 notifications returned as undeliverable may take some reasonable time to search for correct, current addresses for the affected individuals, but must provide substitute notice "as soon as reasonably possible" and within the original 60-day time frame for notifications.



Modification to the Breach Notification Rule: Notification to the Media

- The Secretary clarified several points regarding media notifications, including:
  - Covered entities are not obligated to incur the cost of any media broadcast regarding the breach in question.
  - Media outlets are not obligated to publicize each and every breach notice they receive (and a failure to publicize does not render the notice provided insufficient).
  - Entities must deliver a press release directly to the media outlet being notified. Posting a general press release on a website, for instance, is insufficient.

Modification to the Breach Notification Rule: Response to Additional Public Comments

Though it did not result in a change to any regulatory text, the Final Rule noted that "[b]ecause every breach of unsecured protected health information must have an underlying impermissible use or disclosure under the Privacy Rule, OCR also has the authority to impose a civil money penalty for the underlying Privacy Rule violation, even in cases where all breach notifications were [timely, compliantly] provided."

This statement clarifies that every breach carries with it the potential for OCR enforcement and civil penalties, regardless of the size or circumstances.

Modifications to the HIPAA Privacy Rule Under GINA

The Final Rule finalizes proposed regulatory provisions implementing changes to HIPAA as a result of the Genetic Nondiscrimination Act of 2008 (GINA). These rule changes were first proposed in October 2009.

- The Proposed Rule is, for the most part, adopted without changes, with one exception: the Proposed Rule's expansion of entities covered by the changes (which included all health plans subject to the Privacy Rule) has been modified to exclude issuers of long-term-care policies.
- This change reflects the fact that several comments were received indicating that long-term-care insurance may become financially infeasible without a reliance on genetic information to predict future health conditions. Each regulatory section adopted with noteworthy changes or guidance is discussed below.

Modifications to the HIPAA Privacy Rule Under GINA

The Final Rule adopts the expanded application of the GINA provisions to all health plans subject to HIPAA but notably excludes issuers of long-term-care insurance.

- OCR responded specifically to claims that such an expansion was beyond its authority, noting that it has broad authority to regulate the use and disclosure of health information, including genetic information, in the interest of individuals' privacy.
- The current decision to exclude long-term-care issuers, however, may not be permanent; the Final Rule notes that OCR will be conducting additional studies of the issue, including a study by the National Association of Insurance Commissioners (NAIC), and will reassess the inclusion of long-term-care issuers in the future.