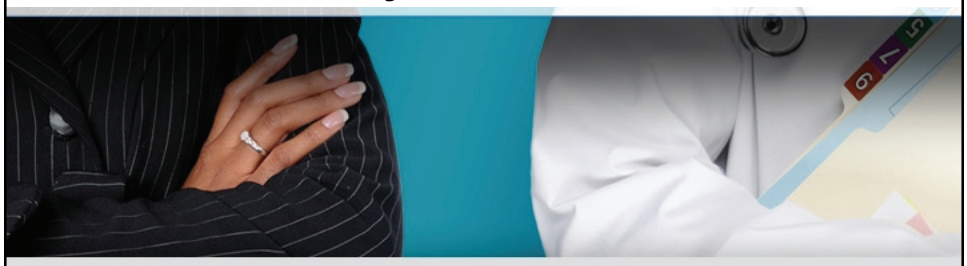
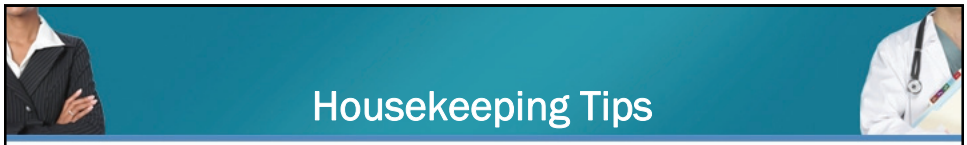
Preparing to Comply With the HITECH Final Rule
Tuesday, March 19, 2013



FOLEY

FOLEY & LARDNER LLP

12.9135



Housekeeping Tips

- Call 888.569.3848 for technology assistance/Dial ***0** (star/zero) for audio assistance.
- Time for live Q&A may be available at the end of the formal presentation. Or questions can be entered at any time via the Q&A pod located on right side of your screen. We will address all questions at the end of the program, time permitting.
- To maximize the presentation Click on the **Full Screen** button located above the presentation slides
- Click on the **Download Files** button located to the right of the presentation slides to get a copy of the slides
- Foley will apply for CLE credit after the Web conference. If you did not supply your CLE information upon registration, please e-mail it to zrahim@foley.com

NOTE: Those seeking **New York & New Jersey CLE** credit are required to complete the Attorney Affirmation Form. A 5-digit code will be announced during the presentation. Email the code to **zrahim@foley.com** to get a copy of the form. Immediately fill it out and return it after the program.

12.9135

Speakers

Mike Scarano
Partner
Foley & Lardner LLP
mscarano@foley.com

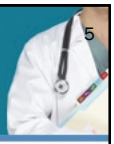
Mike Woolever
Partner
Foley & Lardner LLP
mwoolever@foley.com

Leeann Habte
Associate
Foley & Lardner LLP
lhabte@foley.com

HHS Omnibus Rule

- Implementing regulations for
  - Health Information Technology for Economic and Clinical Health (HITECH) Act &
  - Genetic Information Nondiscrimination Act (GINA)
  - Makes other changes to the Health Insurance Portability and Accountability Act (HIPAA) regulations
- Published: January 25, 2013
- Compliance Date: September 23, 2013
- Compliance Date for Existing Business Associate Agreements: September 22, 2014

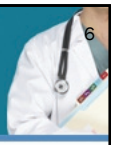
Overview of Changes to HIPAA



5

- Expands the definition of Business Associates
- Makes all Business Associates directly subject to regulatory requirements and enforcement
- Requires changes in Business Associate Agreements
- Changes the "risk analysis" for determination of a breach
- Introduces a presumption of a breach

Overview of Changes to HIPAA



6

- New requirements applicable to marketing, sale of Protected Health Information (PHI), and fundraising
- Relaxes the rules applicable to authorizations for research
- Provides a right to restrict disclosures to health plans under certain circumstances
- Requires changes in Notice of Privacy Practices (NPP) reflecting these changes

Overview of Changes to HIPAA

- Provides individuals with the right to obtain electronic PHI in an electronic format
- Permits disclosure of immunization records to schools without full blown authorization
- Changes definition of PHI to address genetic information and decedents
- Strengthens the rules governing enforcement

Additional Entities are Business Associates

- Health Data transmission organizations, including health information organizations
  - Must be more than a mere conduit; must routinely access PHI in the course of performing their BA duties
- E-prescribing gateways
- Personal health record vendors who manage the health records of covered entities
- Subcontractors include all downstream Subcontractors who have access to PHI

Subcontractors as BAs

- Subcontractor is a person or entity
  - who is not a member of the workforce
  - to whom a business associate delegates a function, activity, or service and
  - will access PHI in the course of performing same
- Business Associate duties of Subcontractors extend to all downstream Subcontractors

Who Contracts with Whom?

- CEs must have business associate agreements with their direct business associates
- Business associates must have BAAs with their Subcontractors
- CEs do not need BAAs with Subcontractors but should be third party beneficiaries of the downstream BAAs

Application of HIPAA to Business Associates

- Business Associates directly subject to applicable HIPAA regulations and to civil and criminal penalties for violations.
  - Direct liability attaches, regardless of whether the entities have entered into a Business Associate Agreement.
- Business Associates are subject to Security Rule.
  - Administrative, physical, and technical safeguards.
  - Written policies and procedures.
  - Security officer
- Subject to certain provisions of Privacy Rule

Business Associate Agreements

- Covered Entities must amend Business Associate Agreements to address new obligations:
  - Compliance with HIPAA Security Rule.
  - Contracts with downstream Subcontractors must include agreement to comply with HIPAA regulations with respect to PHI.
  - Breach reporting to Covered Entity.
- BAAs should contemplate:
  - Costs and liabilities associated with Subcontractors' security breaches or other violations of contract terms related to information security.
  - Breach reporting procedures.
- Consider recommended provisions in OCR's new model BAA language.

Transition Provisions for BAAs Only!

- Allow Covered Entities and Business Associates (including Subcontractors) to continue to operate under certain existing contracts until September 22, 2014.
- Transition Period Applies if
  - Prior to January 25, 2013, the Covered Entity or Business Associate had an existing contract or other written arrangement with a Business Associate or Subcontractor that
    - Complied with the prior provisions of the HIPAA Rules, and
    - Such contract or arrangement was not renewed or modified between March 26, 2013 and September 23, 2013.

Liability of CEs for Violations by their BAs (or of BAs for their downstream BAs)

- A CE is liable for the violations of a BA that meets the definition of "agent" under federal common law
  - The most important criterion is the right to exercise control over the BA
  - In drafting the underlying agreement and the BAA, consider the tradeoff between the need to control the BA and the benefit of not having control

Changes to Breach Reporting Rule

- Existing rule: Report required for breach of unsecured PHI which creates a substantial risk or financial, reputational or other harm to an individual (the so-called "harm standard")
- New rule: Report required unless the CE can demonstrate there is a low probability that the information was compromised
  - More objective and likely to lead to more frequent reports

Breach Notification

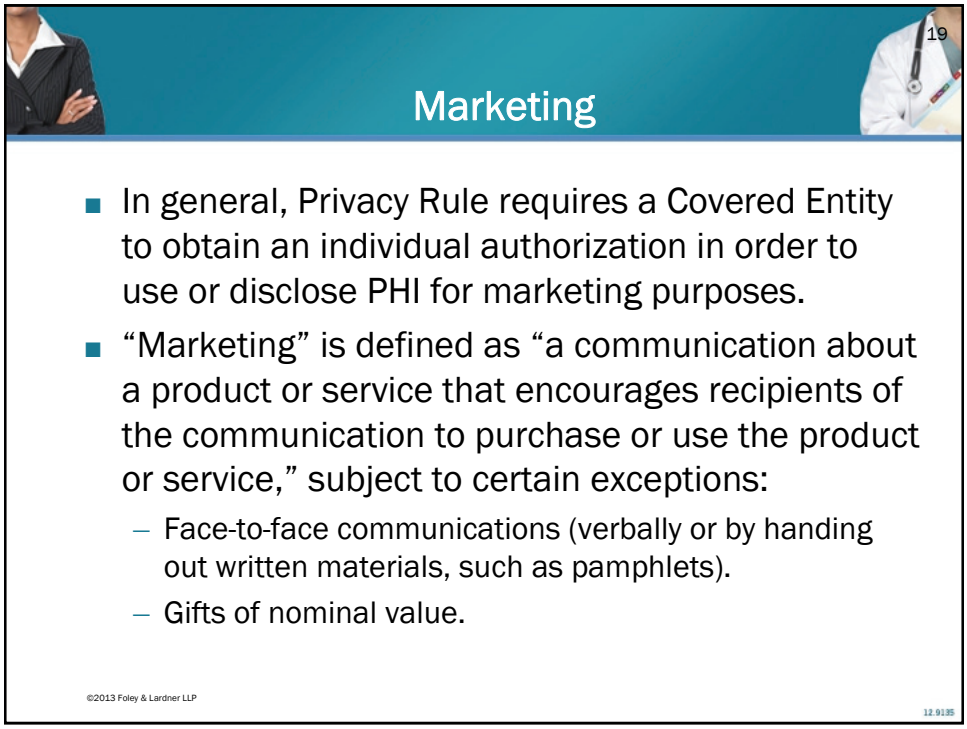
- Impermissible use or disclosure or Security Incident presumed to be Breach
- Burden on the entity to demonstrate low probability of compromise through risk assessment
- Risk Assessment must be
  - Thorough
  - Completed in good faith
  - Have reasonable conclusions
- Discretion to provide notification without performing risk assessment

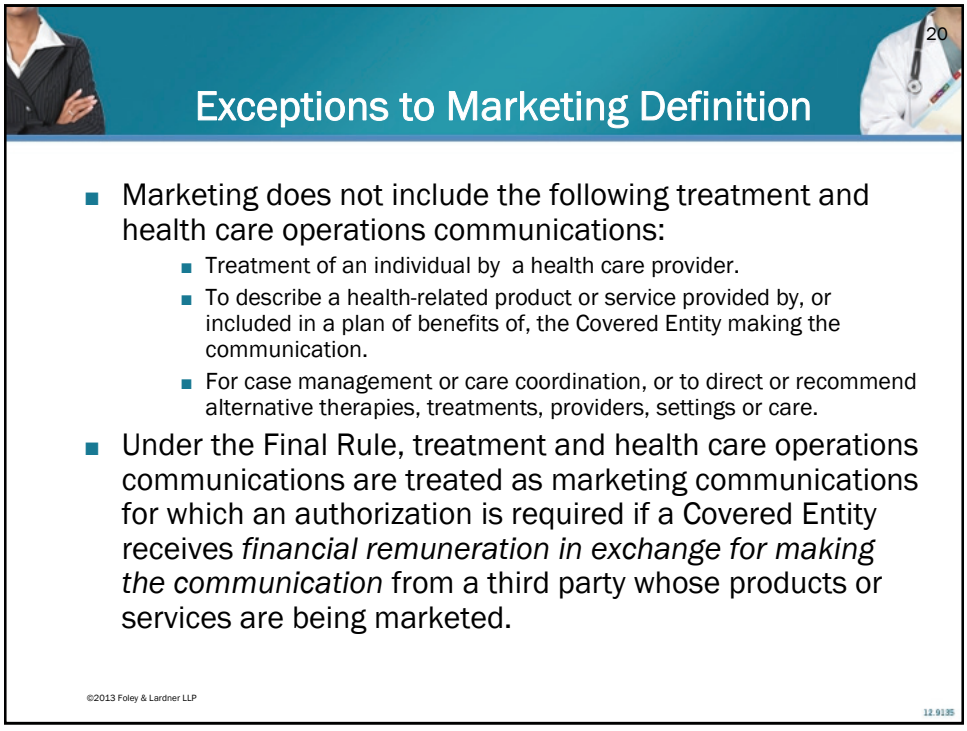
Four Part Risk Assessment for Determining Whether the PHI was Compromised

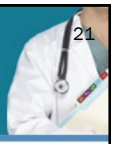
- The nature and extent of the PHI involved
- The individual who impermissibly used the PHI or to whom the impermissible disclosure was made
- Whether the PHI was actually acquired or viewed, or if only the opportunity existed for the information to be acquired or viewed
- The extent to which the risk to the PHI has been mitigated

Risk Assessment

- Many questions remain, particularly since there now is no definition of "compromise the PHI"
  - Webster's Dictionary: "a laying open to danger, suspicion, or disrepute; to endanger the interests of."
- Considerable uncertainty about how to weight factors in the four part analysis"
- Guidance promised

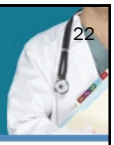

19
Marketing
In general, Privacy Rule requires a Covered Entity to obtain an individual authorization in order to use or disclose PHI for marketing purposes.
"Marketing" is defined as "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service," subject to certain exceptions:
Face-to-face communications (verbally or by handing out written materials, such as pamphlets).
Gifts of nominal value.
©2013 Foley & Lardner LLP


20
Exceptions to Marketing Definition
Marketing does not include the following treatment and health care operations communications:
Treatment of an individual by a health care provider.
To describe a health-related product or service provided by, or included in a plan of benefits of, the Covered Entity making the communication.
For case management or care coordination, or to direct or recommend alternative therapies, treatments, providers, settings or care.
Under the Final Rule, treatment and health care operations communications are treated as marketing communications for which an authorization is required if a Covered Entity receives financial remuneration in exchange for making the communication from a third party whose products or services are being marketed.
©2013 Foley & Lardner LLP



Revised Framework for Marketing

- Definition of "financial remuneration":
  - Direct or indirect payment from or on behalf of third party whose product or service is being described.
    - Does not include payment for treatment.
    - Does not include in-kind benefits.
- Authorization must state that financial remuneration is involved.
  - Scope of authorization is not limited to a single product or service.



Revised Marketing Restrictions

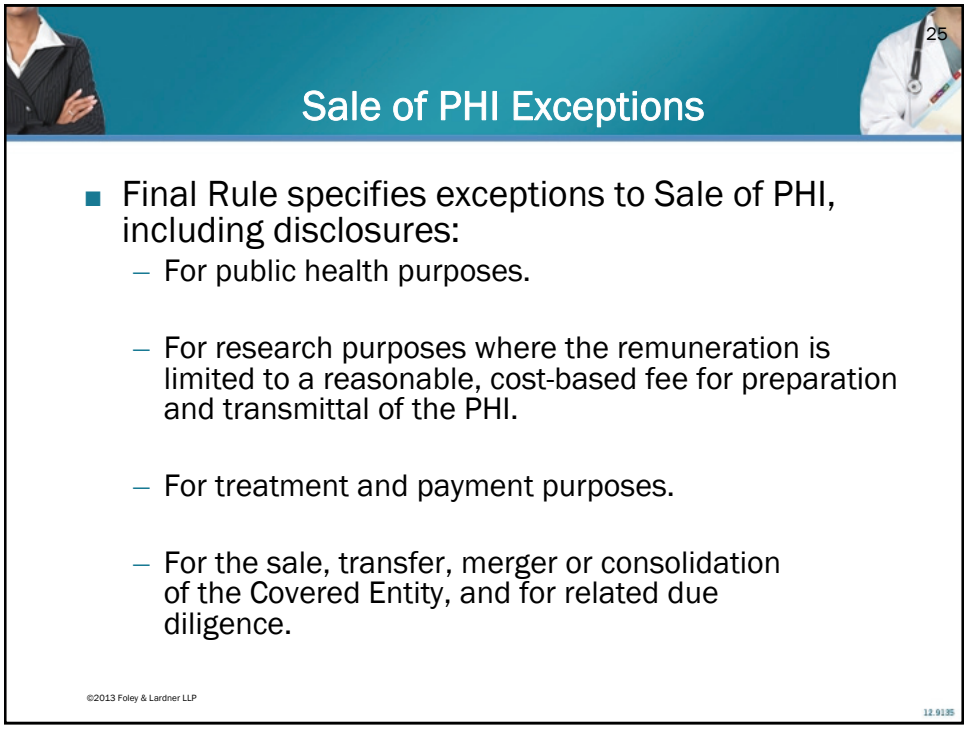
- Exception for communications to provide *refill reminders* or otherwise communicate about a drug or biologic being prescribed for an individual provided that any *financial remuneration* received is *reasonably related to costs* of making the communication (labor, supplies, & postage).
  - Exception includes
    - Communications about generic equivalent of a drug being prescribed to an individual.
    - Adherence communications.
    - Prescriptions for self-administered drugs or biologics.

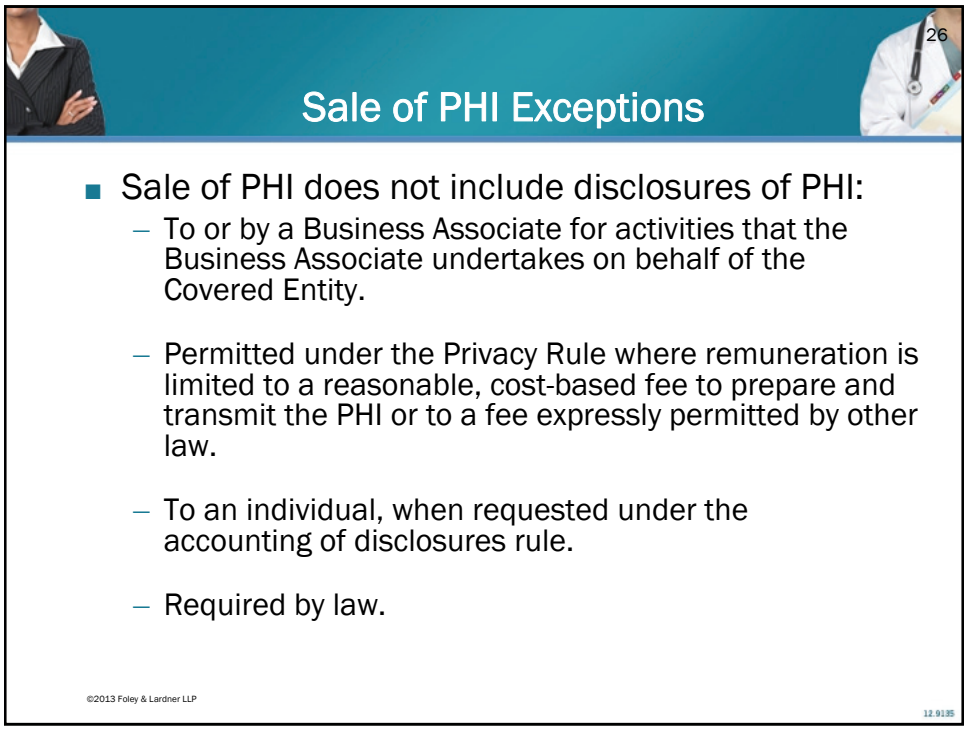
Compliance

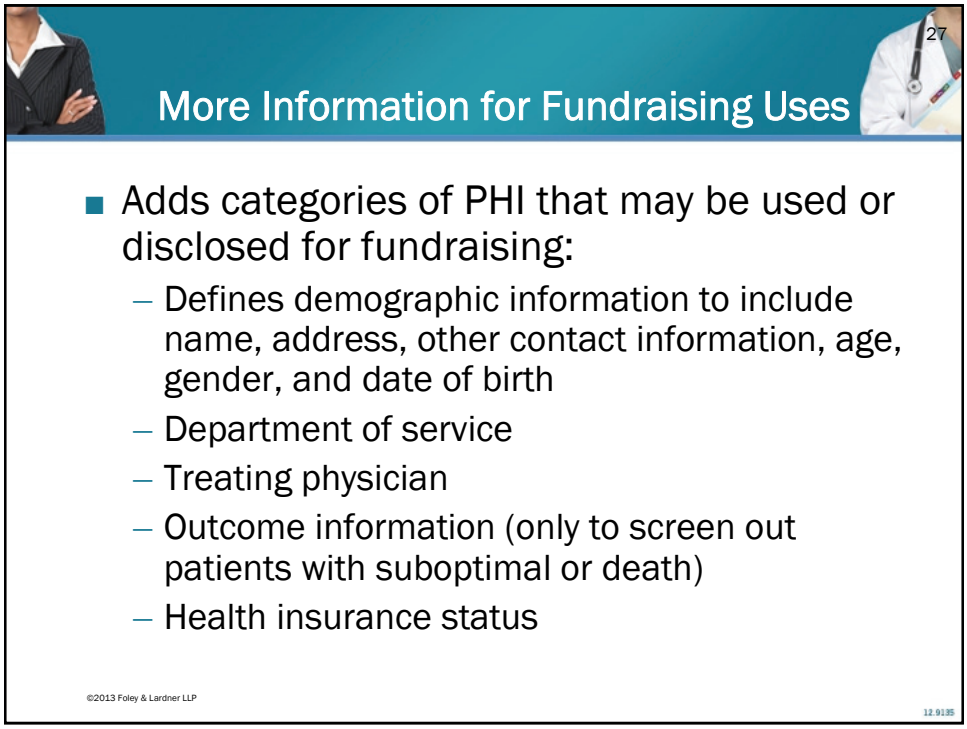
- The Final Omnibus Rule restricts previously permissible subsidized communications about the health-related products and services of a third party without patient authorization.
- Covered Entities should:
  - Review their contracts and other arrangements with third parties to ensure compliance with new requirements.
  - Revise authorizations for marketing purposes.

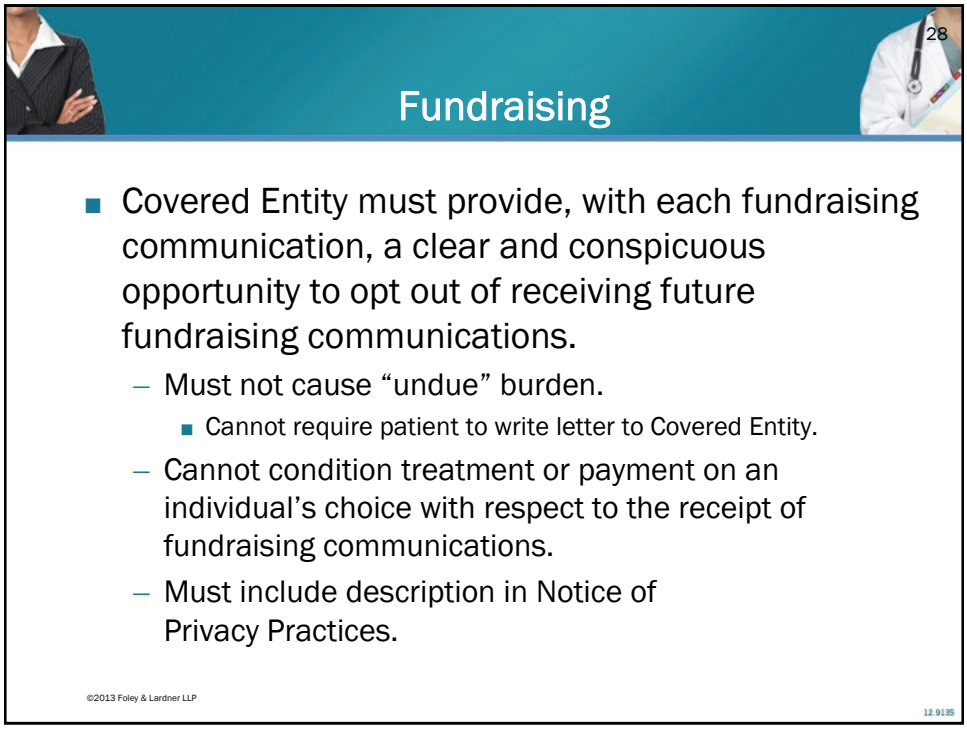
Sale of PHI

- Final Omnibus Rule prohibits a Covered Entity or Business Associate from receiving direct or indirect remuneration for the disclosure of PHI without an individual authorization.
- Requires that the individual authorization state that the disclosure will result in remuneration to the Covered Entity.


25
Sale of PHI Exceptions
Final Rule specifies exceptions to Sale of PHI, including disclosures:
For public health purposes.
For research purposes where the remuneration is limited to a reasonable, cost-based fee for preparation and transmittal of the PHI.
For treatment and payment purposes.
For the sale, transfer, merger or consolidation of the Covered Entity, and for related due diligence.
©2013 Foley & Lardner LLP


26
Sale of PHI Exceptions
Sale of PHI does not include disclosures of PHI:
To or by a Business Associate for activities that the Business Associate undertakes on behalf of the Covered Entity.
Permitted under the Privacy Rule where remuneration is limited to a reasonable, cost-based fee to prepare and transmit the PHI or to a fee expressly permitted by other law.
To an individual, when requested under the accounting of disclosures rule.
Required by law.
©2013 Foley & Lardner LLP


27
More Information for Fundraising Uses
Adds categories of PHI that may be used or disclosed for fundraising:
Defines demographic information to include name, address, other contact information, age, gender, and date of birth
Department of service
Treating physician
Outcome information (only to screen out patients with suboptimal or death)
Health insurance status
©2013 Foley & Lardner LLP

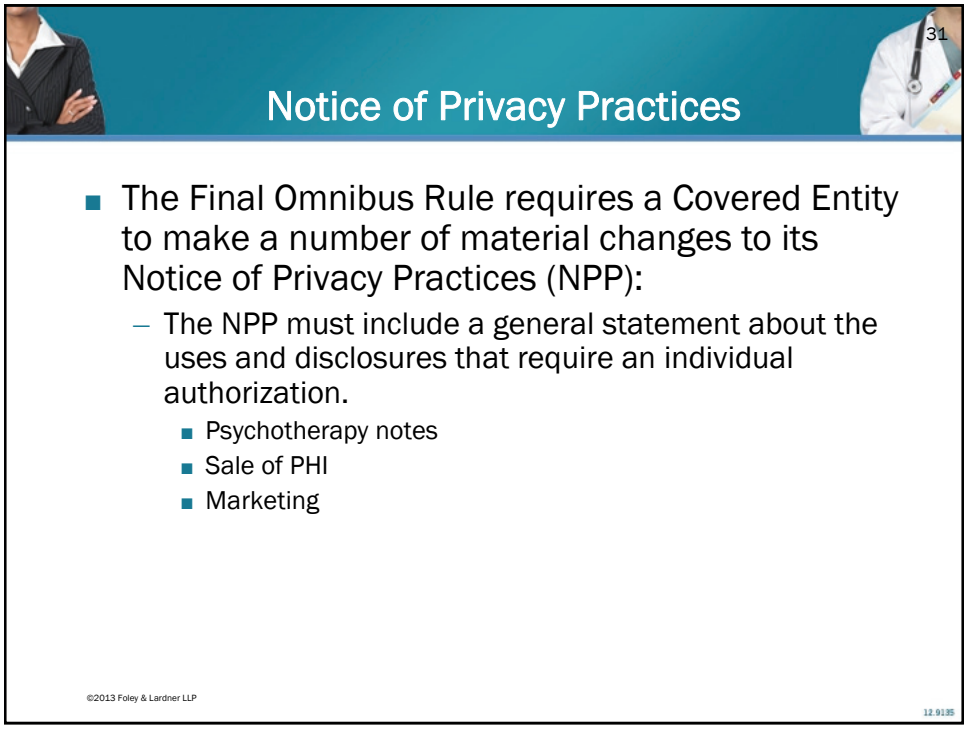

28
Fundraising
Covered Entity must provide, with each fundraising communication, a clear and conspicuous opportunity to opt out of receiving future fundraising communications.
Must not cause "undue" burden.
Cannot require patient to write letter to Covered Entity.
Cannot condition treatment or payment on an individual's choice with respect to the receipt of fundraising communications.
Must include description in Notice of Privacy Practices.
©2013 Foley & Lardner LLP

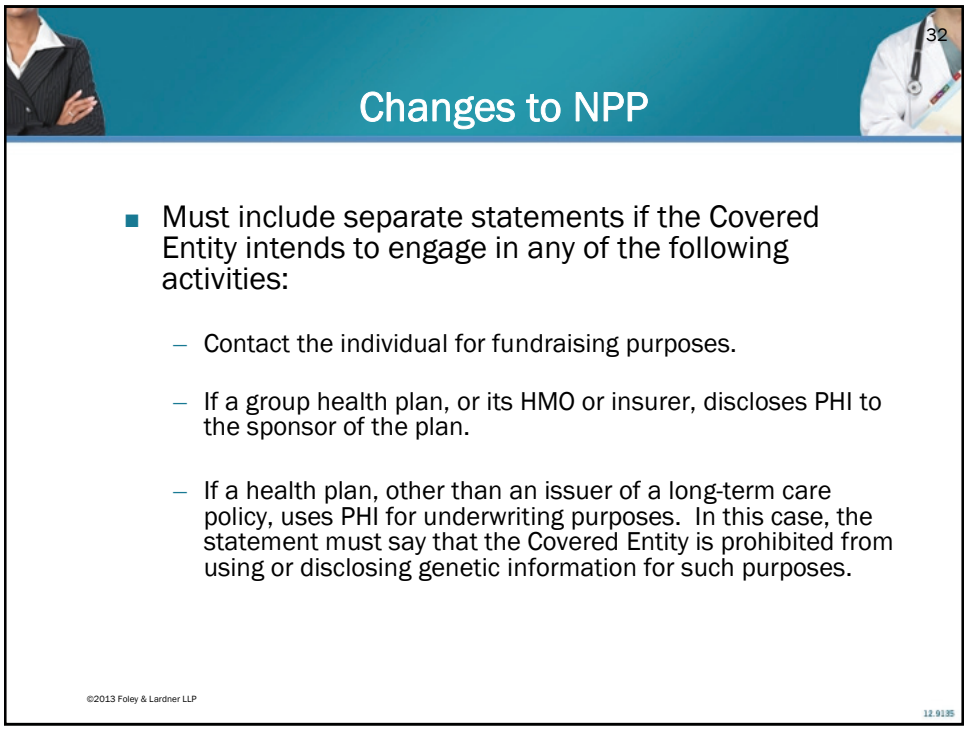
Fundraising

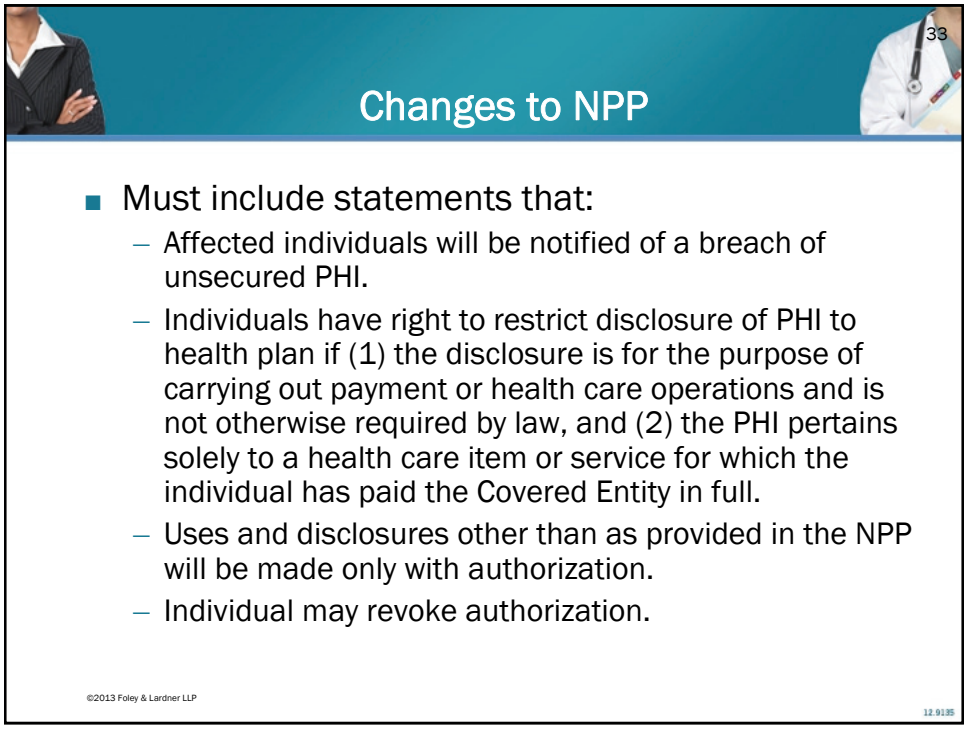
- When an individual has opted out of receiving fundraising communications, a Covered Entity may not continue to send the individual such communications.
  - Previous standard was "reasonable effort".
- Covered Entity may provide method for individual to opt back in.

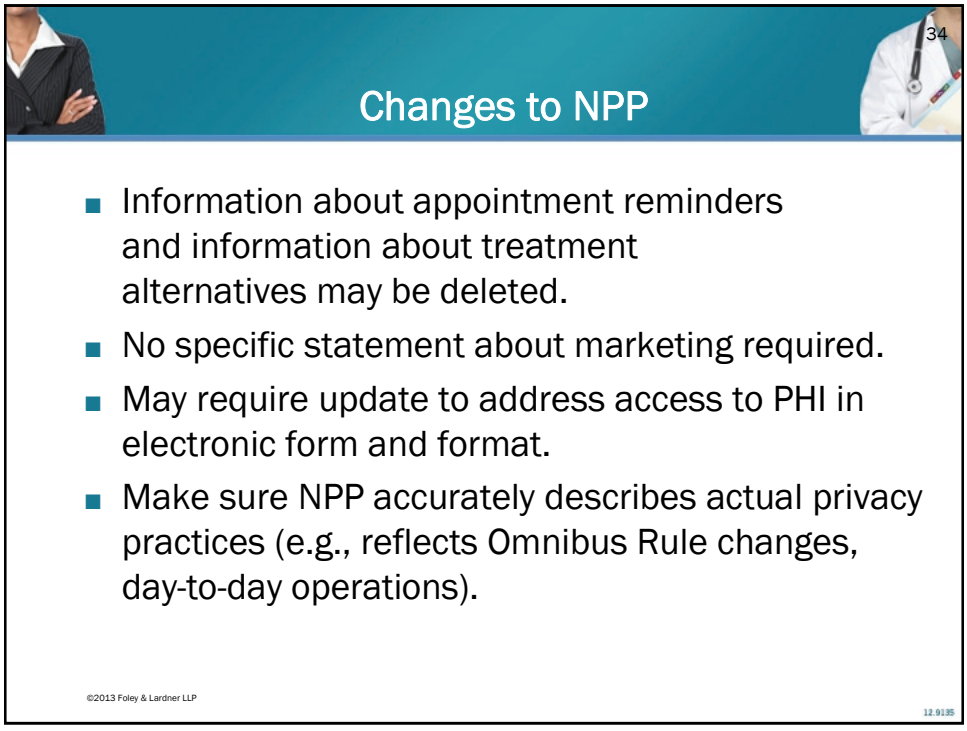
Compliance

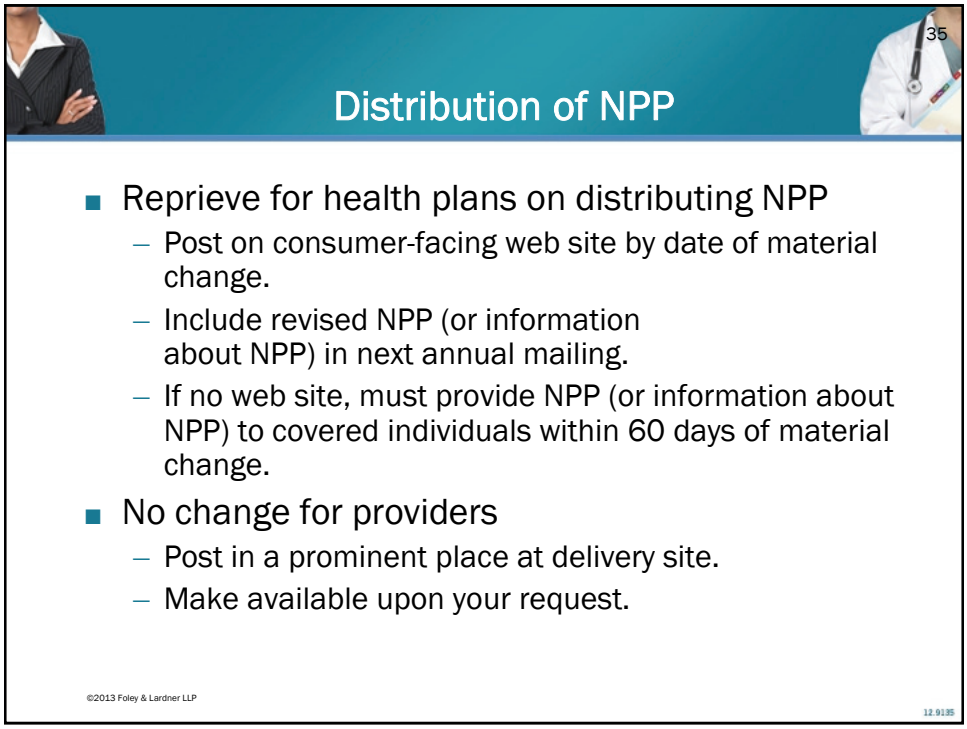
- Consider targeted fundraising options available with additional data elements.
- Design new opt-out methods and develop opt-out language for fundraising communications.
  - 800 number, e-mail, pre-paid post cards.
- Consider whether to allow opt-in.
- Develop data management systems to track opt-outs and opt-ins.
- Revise Notice of Privacy Practices.

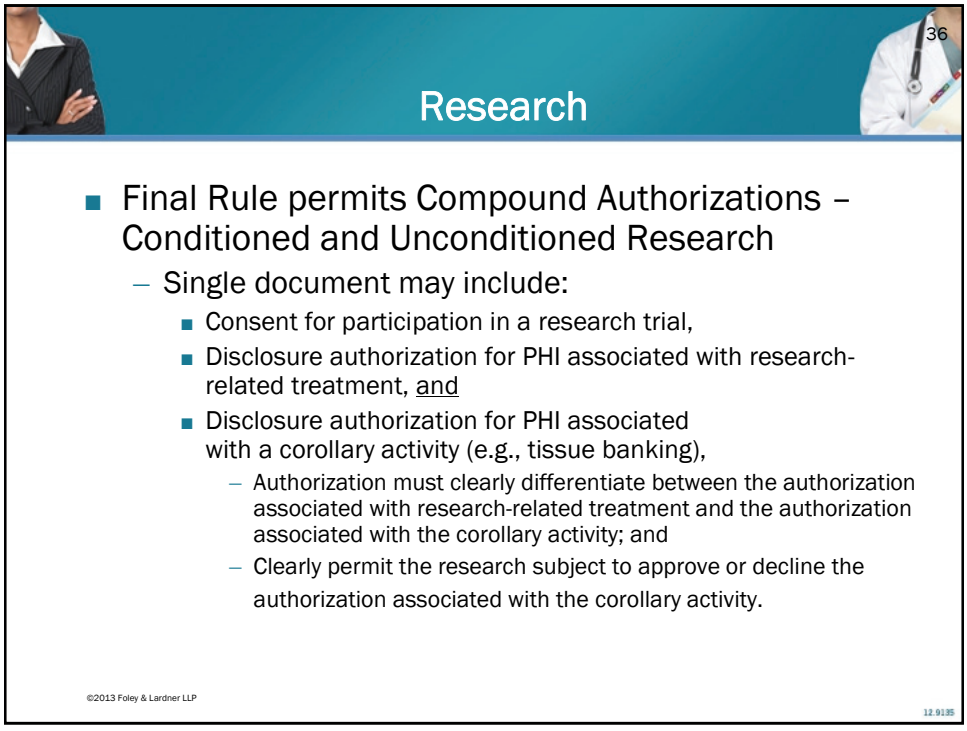

31
Notice of Privacy Practices
The Final Omnibus Rule requires a Covered Entity to make a number of material changes to its Notice of Privacy Practices (NPP):
The NPP must include a general statement about the uses and disclosures that require an individual authorization.
Psychotherapy notes
Sale of PHI
Marketing
©2013 Foley & Lardner LLP


32
Changes to NPP
Must include separate statements if the Covered Entity intends to engage in any of the following activities:
Contact the individual for fundraising purposes.
If a group health plan, or its HMO or insurer, discloses PHI to the sponsor of the plan.
If a health plan, other than an issuer of a long-term care policy, uses PHI for underwriting purposes. In this case, the statement must say that the Covered Entity is prohibited from using or disclosing genetic information for such purposes.
©2013 Foley & Lardner LLP


33
Changes to NPP
Must include statements that:
Affected individuals will be notified of a breach of unsecured PHI.
Individuals have right to restrict disclosure of PHI to health plan if (1) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law, and (2) the PHI pertains solely to a health care item or service for which the individual has paid the Covered Entity in full.
Uses and disclosures other than as provided in the NPP will be made only with authorization.
Individual may revoke authorization.
©2013 Foley & Lardner LLP


34
Changes to NPP
Information about appointment reminders and information about treatment alternatives may be deleted.
No specific statement about marketing required.
May require update to address access to PHI in electronic form and format.
Make sure NPP accurately describes actual privacy practices (e.g., reflects Omnibus Rule changes, day-to-day operations).
©2013 Foley & Lardner LLP


35
Distribution of NPP
Reprieve for health plans on distributing NPP
Post on consumer-facing web site by date of material change.
Include revised NPP (or information about NPP) in next annual mailing.
If no web site, must provide NPP (or information about NPP) to covered individuals within 60 days of material change.
No change for providers
Post in a prominent place at delivery site.
Make available upon your request.
©2013 Foley & Lardner LLP


36
Research
Final Rule permits Compound Authorizations – Conditioned and Unconditioned Research
Single document may include:
Consent for participation in a research trial,
Disclosure authorization for PHI associated with research-related treatment, and
Disclosure authorization for PHI associated with a corollary activity (e.g., tissue banking),
Authorization must clearly differentiate between the authorization associated with research-related treatment and the authorization associated with the corollary activity; and
Clearly permit the research subject to approve or decline the authorization associated with the corollary activity.
©2013 Foley & Lardner LLP

Research

- Final Rule permits disclosure authorizations for future research
  - Current authorizations must be study-specific (thereby limiting an individual's ability to agree to the use or disclosure of their PHI for future research without having to be re-contacted to sign additional authorization forms in the future).
  - Final Rule permits an individual to authorize disclosure of PHI for future research if such purposes are adequately described so as to put the individual on notice that his or her PHI could be used or disclosed for such future research.

Immunization Records

- Immunizations
  - Covered Entities may disclose proof of immunization to schools in States that have laws requiring proof of immunization without written authorization, but oral agreement and documentation of agreement is necessary.
- Access to PHI
  - Covered Entities must provides access to PHI in electronic form or format if PHI is maintained electronically in the form or format requested, or if unavailable in a form and format mutually agreeable to the parties.
  - May charge reasonable labor and supply costs (if any) incurred in producing the electronic or paper copy, plus postage (if any).
- Decedents
  - PHI excludes individually identifiable information of a person who has been deceased for more than 50 years.
  - Covered Entities may disclose decedent's information to family members and other who were involved in the care or payment for care of the decedent prior to death, unless it contradicts a prior expressed preference known to the Covered Entity

Compliance

- Review existing policies against OCR's audit protocol.
- Revise NPP and make available.
- Revise marketing, fundraising, sale of PHI, research, uses and disclosures, access to PHI, and related policies.
- Implement procedures to incorporate revisions.
- Determine implementation schedule.

GINA-Related Changes

- The Final Rule modifies the Privacy Rule as directed by the Genetic Information Nondiscrimination Act of 2008 ("GINA").
  - The Final GINA Rule adopts an October 2009 Proposed Rule with limited changes.
  - The Final GINA Rule adopts the same September 23, 2013 compliance date as the Final HITECH Rule.

GINA-Related Changes

- GINA prohibits discrimination based on an individual's genetic information in both health coverage and employment.
- With respect to employment, GINA –
  - Prohibits the use of genetic information in the employment context (e.g., hiring and firing);
  - Restricts employers from requesting, requiring or purchasing genetic information; and
  - Limits the disclosure of genetic information.

GINA-Related Changes

- With respect to health coverage, GINA -
  - Prohibits discrimination in eligibility or premiums/ contributions based on genetic information (ERISA §702(a) and (b)); and
  - Prohibits insurers and group health plans from using genetic information for underwriting purposes, collecting genetic information prior to enrollment, or requesting or requiring genetic tests (ERISA § 702(c) and (d)).
  - Violations are subject to a $100 per day per participant per violation excise tax under Code Section 4980D (Code Section 9802).

GINA-Related Changes

- GINA also expressly directed HHS to amend the Privacy Rule to –
  - Clarify that genetic information is health information; and
  - Provide that the use of genetic information by a group health plan, health insurance issuer, or Medicare supplement insurer for underwriting purposes was not a permitted use or disclosure under the Privacy Rule; and
  - Incorporate the GINA definitions of the terms "genetic information", "genetic test" and "family member" in the Privacy Rule.
  - See 42 U.S.C. 1320d-9.

GINA-Related Changes

- Genetic Information as Health Information
  - HHS issued informal guidance in 2002 that health information includes genetic information for privacy purposes without defining what was included in "genetic information".
  - GINA filled in the blanks by providing key definitions and directing HHS to amend the Privacy Rule based on the GINA definitions.
  - The Final Rule completes the regulatory circle by formally incorporating the GINA definitions (from both the statute and regulations) and requirements into the Privacy Rule.

GINA-Related Changes

- Definitions in the Final Rule are consistent with the definitions in GINA and the GINA non-discrimination regulations.
- "Genetic Information" includes
  - An individual's genetic tests;
  - Genetic tests of family members;
  - The manifestation of a disease or disorder in a family member; and
  - Any request for, or receipt of, genetic services or participation in clinical research that includes genetic services by an individual or family member;
  - But not, an individual's age or sex.

GINA-Related Changes

- "Genetic test" means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites to detect genotypes, mutations, or chromosomal changes.
  - But not an analysis that is directly related to a manifested disease, disorder or pathological condition
  - A disease, disorder or pathological condition is manifested if it has been or reasonably could be diagnosed by a health care professional with appropriate training.

GINA-Related Changes

- "Genetic services" includes genetic tests, as well as genetic counseling (including obtaining, interpreting, or assessing genetic information) and education.
  - Note, not only the results of genetic tests, but also the fact that an individual sought or received a genetic test or genetic counseling or education is protected information.

GINA-Related Changes

- A "family member" includes not only dependents, but also relatives through the fourth degree (i.e. great-great grand parents or great-great grand children and children of first cousins).
  - Includes relatives by affinity (marriage or adoption) and consanguinity (common biological ancestor);
  - Includes a fetus and any embryo legally held using assisted reproductive technology;
  - Partial and full consanguinity treated the same (full and half-siblings).

GINA-Related Changes

- GINA prohibits the use or disclosure of genetic information for underwriting purposes by a group health plan, health insurance issuer, or issuer of a Medicare supplement policy.
- Final Rule applies prohibition to all "health plans" subject to the Privacy Rule, not just those mentioned in GINA;
  - "health plan" includes an individual or group plan that provides, or pays the cost of, medical care, including –
    - A group health plan, health insurer, HMO, Medicaid, Medicare, FEHP, and state risk pools;
    - Note that the "health plan" definition also includes limited scope dental and vision and other medical care "excepted benefits".
  - Long term care insurance is excepted from the GINA underwriting rule (subject to further study), but not the other provisions of the Privacy Rule.

GINA-Related Changes

- "Underwriting purposes" is broadly defined consistent with the GINA non-discrimination rules to include –
  - Rules for, or determination of, eligibility or benefits;
    - Including changes in cost-sharing in return for activities (e.g. completing risk assessment or participating in wellness program)
  - Computing premiums or contribution amounts;
  - Applying pre-ex rules; and
  - Other activities related the creation, renewal, or replacement of insurance or health benefits.
  - But not, whether a service is medically appropriate.

GINA-Related Changes

- Covered entities are not prohibited from using health information that is not genetic information for underwriting purposes (subject to other requirements under HIPAA/ACA market reform rules).
- *But NPP Revision Required - if a health plan uses PHI for underwriting purposes its Notice of Privacy Practices must affirmatively state that it is prohibited from using genetic information for such purpose.*

Questions?

- Mike Scarano – mscarano@foley.com
- Leeann Habte – lhabte@foley.com
- Mike Woolever – mwoolever@foley.com