Practical Guidance and Proposed Solutions in Response to the HIPAA Final Omnibus Rule

February 21, 2013

Megan Hardiman
Katten Muchin Rosenman LLP
Chicago, Illinois
312.902.5488
megan.hardiman@kattenlaw.com

Michael R. Callahan
Katten Muchin Rosenman LLP
Chicago, Illinois
312.902.5634
michael.callahan@kattenlaw.com

Katten
Katten Muchin Rosenman LLP

Final Rule Overview, Breach and Business Associates

Megan Hardiman

Final Rule Overview

- Breach Notice
  - Eliminates “significant risk of harm” threshold for breach notification
  - Changes the risk assessment process

Final Rule Overview

- Significant impact on BAs
  - Implementing BA's directly liability for compliance with certain HIPAA Privacy and Security Rules requirements
  - Expands definition of BAs to include subcontractors
  - Mandates new content for business associate agreements

Final Rule Overview

- Numerous Privacy and Security Rule Changes:
  - Stronger limits on marketing
  - Increased flexibility for fundraising
  - Prohibition on sale of PHI
  - More flexibility for research authorizations
  - Flexibility on sharing decedents information with those involved in care

Final Rule Overview

- Modifies content of the Notice of Privacy Practices ("NPP"); distribution requirements
- Implements an individual's right to restrict certain disclosures to PHI to a health plan
- Enhances an individual's right to access an electronic copy of PHI

- Generally prohibits CE health plans from using or disclosing genetic information for underwriting purposes
- Further strengthens enforcement

Key Compliance Dates

- Final Rule
  - Published January 25, 2013
  - Effective March 26, 2013
  - *General* compliance deadline September 23, 2013
    - Certain exceptions

Breach Notification- Key Changes

- Eliminates the “significant risk of harm” threshold
- The “default” mode of the rule is notification.
  - *Any* impermissible use or disclosure of PHI is presumed to be a breach requiring notification *unless*
    - The CE or BA demonstrates via a risk assessment that there is a **“low probability that the PHI has been compromised”** or
    - One of the Rule’s narrow exceptions applies.

Katten
Katten Muchin Rosenman LLP

Breach Notification- A More "Objective" Risk Assessment

- Any risk assessment **must** consider at least the 4 following factors; it **may** consider others.
- If the assessment fails to demonstrate "low probability of compromise", **you must notify**.
- Can we skip the risk assessment and go straight to notice?

Breach Notification – Risk Assessment

1. Nature and Extent of PHI Involved
   - What types of *identifiers*?
   - Did it include more *sensitive* types of info?
   - What is the *likelihood of re-identification*?

Breach Notification – Risk Assessment

2. Nature of the Recipient

- Was the recipient subject to HIPAA Rules? Federal agency obligated to comply with various privacy laws?
- If the PHI disclosed is *not immediately identifiable,* does the recipient have the ability to re-identify the information?

Breach Notification- Risk Assessment

3. Was PHI Actually Acquired or Viewed?

- Or was there just an opportunity to do so?

Breach Notification- Risk Assessment

4. Has the risk been mitigated?
   - To what extent has risk of compromise been mitigated?
     - What steps were taken?
   - How effective is the mitigation?
     - Consider the recipient

Katten
Katten Muchin Rosenman LLP

Breach Notification- Removal of Limited Data Set Exception

- HHS removed the exception to breach notice for limited data sets that do not contain any dates of birth and zip codes.

Breach Notification- Clarifications on Notice

- **Breach at or by a BA.** CE ultimately has the obligation of notice. It can be delegated.
- **Alternative Addresses Upon Request.** Rule does not prohibit a CE from sending a breach notice to an alternative address rather than a home address (i.e., work) where individual requests communications be sent to such address.
- **Highly confidential communications option.** If individual has agreed only to receive communications from a provider orally or by phone, the provider may call the individual to request and have the individual pick up written breach notice from provider directly. If individual can't/won't, can provide all notice info on phone and document this. Department will exercise enforcement discretion.

Breach Notification- Clarifications on Notice

- **Plan Participants at Same Address.** Sending one notice addressed to both plan participant and participant's spouse or dependents under the plan affected by the breach is allowed, if they all reside at same address and CE identifies clearly who is affected by the breach.
  - Must have same address
  - For dependents, the plan participant/spouse must be personal reps
- **Notice to Secretary of "Small" Breaches from Prior Year**. CEs are required to notify the HHS Secretary of all breaches of unsecured PHI affecting *fewer than 500 individuals* not later than 60 days after the end of the calendar year in which the breaches were "discovered," and not in which the breaches "occurred."
  - Still need to report to individual without unreasonable delay and no later than 60 days after discovery.

Breach Notification- Breach By Subcontractor

- A Business Associate Agreement must require subcontractors who handle e-PHI to report security incidents and breaches to the business associate with which it contracts.

Katten
Katten Muchin Rosenman LLP

Breach Notification- Practical Considerations

- Update your breach notice policies to reflect changes
  - "Risk of harm" standard is out
  - Risk assessment factors are in
- Document and maintain risk assessment/notices
  - CEs and BAs continue to have the burden of proof re: notices provided or no breach
    - Good faith, thorough, reasonable

Breach Notification- Practical Considerations

- Contractual Considerations
  - Timing of notice provisions
    - Timing is collapsed if a BA is your “agent”
    - Identify agents and develop a strategy to manage “agent” risks
  - Indemnification, insurance, etc.

Breach Notification- Practical Considerations

- Expect increased breach notification
  - Encryption “safe harbor”

Business Associates - Overview of Key Changes

- Expands the definition of BAs
- Explains the increased compliance obligations that apply directly to BAs under the HIPAA Rules
- Explains scope of direct liability for HIPAA violations to BAs.
- Identifies required changes to Business Associates agreements.

Business Associates - Who is a BA? An Expanded Definition

- Health information organizations
- E-prescribing gateways
- Others who provide *data transmission services* to a CE and that require *routine access* to such PHI
- HHS clarifies entities that *maintain* PHI on behalf of a CE are BAs, even if they do not actually view the PHI
  - Document storage companies are BAs
- Persons who offer PHRs to individuals "on behalf of" a CE
- Patient safety activities by PSOs
- **Subcontractors**

Business Associates - What is a Subcontractor?

- Any person:
  - ***to whom a BA delegates a function***, ***activity or service***
  - where the delegated function involves the ***creation, receipt, maintenance or transmission of PHI*****,**
  - and who is ***not part of the BA's "workforce***".
- Subcontractors are subject to the same ***compliance obligations and direct liability*** under HIPAA as a first-tier BA.

Business Associates - Not a Subcontractor

- A BA's disclosures of PHI for its ***own management and administration*** or ***legal responsibilities*** do not create a BA relationship with the recipient.
  - The BAA needs to permit these

Business Associates - Scope of BA's Direct Liability

- Impermissible uses and disclosures of PHI
  - Uses and disclosures must comply with the terms of the BA agreement
  - A BA generally can't use or disclosing PHI in any manner that would be impermissible if so done by the CE
    - Exceptions for own proper management/administration/legal responsibilities and data aggregation
      - If permitted by BAA
- Failure to provide breach notification to the CE;

Business Associates - Scope of BA's Direct Liability

- Failure to provide access to a copy of electronic PHI to either the CE, an individual or such individual's designee;
- Failure to disclose PHI when required by the Secretary to investigate or determine the BA's compliance with the HIPAA Rules;
- Failure to provide an accounting of disclosures; and
- Failure to comply with the requirements of the HIPAA Security Rule

Business Associates - Contractual Liability

- BAs remain contractually liable for all other HIPAA Privacy Rule obligations that are included in their contracts or arrangements.

Business Associates - Vicarious Liability for BA "Agents"

- A CE or business associate is vicariously liable for penalties for the failure of its business associate "agent" to perform an obligation on the CE's or BA's behalf.
- When is a BA an "agent"? Federal common law:

Business Associates

- A BA that is aware of non-compliance by its subcontractor must:
  - Take reasonable steps to cure the breach or end the violation; and
  - If such steps were unsuccessful, terminate the contract or arrangement or face liability for non-compliance with the BA requirements.

Business Associates - Business Associate Agreements

- New content requirements:
  - Require the BA to comply, where applicable, with the HIPAA **Security Rule** with regard to electronic PHI;
  - Require the BA to report **breaches** of unsecured PHI to covered entities;
  - Ensure that any **subcontractors** that create or receive PHI on behalf of a BA agree to the same restrictions and conditions that apply to BAs with respect to such information
  - **To the extent the BA is to carry out a CE's obligation under the HIPAA Privacy Rule, the contract must require the BA to comply with the requirements of the HIPAA Privacy Rule that apply to the CE in the performance of such obligation.**
- OCR has posted a sample BAA

Business Associates - Does a CE need to execute BAAs directly with subcontractors?

- No.
- This is the obligation of the BA making the delegation.
- The requirement to obtain a written BA agreement extends down the chain indefinitely.

Business Associates - What if the parties fail to execute a business associate agreement?

- Direct liability still attaches.
  - An entity, ***including a subcontractor***, is a business associate for purposes of HIPAA by virtue of meeting the definition, whether or not there is a written agreement.
- But, the HIPAA Rules require CEs and BAs (including subs) to have a written agreement meeting the requirements.

Katten
Katten Muchin Rosenman LLP

Business Associates - Grandfathering of Existing BAAs

- **If**
  - You had a HIPAA compliant business associate agreement
  - It was in place prior to **January 25, 2013**
  - And you do not renew or modify it from **March 26, 2013**, until **September 23, 2013**
- That BAA is grandfathered until the earlier of (i) the date it is renewed or modified, or (ii) **September 22, 2014**.
- **If not**, then the parties will need to enter into an agreement complying with the Final Rule by **September 23, 2013.**

Business Associates - Practical Considerations

- Identify any new BAs per the new definition
  - Put in place BAAs
- If you are a “new” BA/subcontractor (or even an existing BA)
  - Are you in compliance?
  - How will you get there?
- Identify your “agents”
  - Develop a strategy to manage “vicarious liability” risk

Business Associates - Practical Considerations

- Consider potential breach notification timing issues, especially with agents
- Update your form of BAA
  - New content requirements
    - Which of your BAs are “fulfilling CE responsibilities”
  - Vicarious liability issues
  - Security
  - Indemnifications and insurance

Business Associates - Practical Considerations

- Develop a plan for renegotiating existing BAAs by the applicable deadline
  - Which contracts are grandfathered?
- Contracts with Subs – make sure you are not permitting the sub to do anything you are not permitted to do
  - BAs should ensure they are permitted to use for proper management/legal responsibilities
  - Can you de-identify PHI?

Marketing
Sale of PHI
Fundraising
Access to PHI
Restricting Disclosure of PHI

Sarah Sager Stephanie Goldman

Marketing

- The Final Rule requires authorization for all treatment and health care operations communications where the CE or BA receives financial remuneration for making the communications from a third party whose product or service is being marketed.
- Bright line approach for all subsidized communications that encourage the purchase or use of a health related product or service

Marketing

- "Financial Remuneration"
  - Does not include in-kind benefits
  - Does not include financial remuneration to implement a program as part of CE's services
- Contents of Authorization
  - Must disclose that the CE receives remuneration
  - Individual may revoke at any time
  - May cover subsidized communications generally (as opposed to a single product or product of a single party)

Marketing: Exceptions

- Face to face communication
- Gifts of nominal value
- Refill reminders and Communications about currently prescribed drugs
  - “Reasonable in Amount”
- Communications promoting health in general
- Communications about government-sponsored programs

Marketing: Action Steps

- Policies and procedures should reflect the Final Rule.
- Ensure the authorization contains the required elements.
  - Disclose that the covered entity is receiving financial remuneration from a third party.
  - The scope may apply broadly to subsidized communications in general as long as it adequately describes the purposes of the requested uses and disclosures.
  - Make clear that the individual may revoke at any time.

Sale of PHI: Definitions

- Prohibition on "sale of PHI" without a valid authorization.
- Definition of "sale of PHI."
  - "A disclosure of PHI 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 PHI in exchange for the PHI."
- Definition of "remuneration."
  - Non-financial as well as financial benefits.
- Impact on Research Grants and Health Information Exchanges.

Sale of PHI: Authorization Exceptions

- Exceptions to the authorization requirement:
  - For public health purposes.
  - For research purposes where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost of preparing and transmitting the PHI.
  - For treatment and payment purposes.
  - For the sale, transfer, merger or consolidation of all or part of the covered entity and related due diligence.
  - To or by a business associate for activities that the business associate undertakes on behalf of a covered entity where the only remuneration provided is by the covered entity to the business associate for the performance of such activities.

Sale of PHI: Authorization Exceptions

- To an individual, when requested under the access/accounting of disclosures provisions of HIPAA.
- For disclosures required by law.
- For any other purpose permitted by and in accordance with the applicable requirements of HIPAA, where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by law.

Sale of PHI: Action Steps

- Institute a policy prohibiting the sale of protected health information. Such policy should address:
  - Any applicable exceptions to the prohibition (e.g. receipt of remuneration in exchange for providing an individual access to his or her protected health information).
  - Type of remuneration that can be accepted pursuant to such exceptions (e.g., labor costs and postage).

Fundraising: Available PHI

- Expanded PHI Available for Fundraising
  - Demographic Information
    - Names & Addresses
    - Age
    - Gender
    - Date of Birth
  - Health Insurance Status
  - Dates Health Care Provided

Fundraising: Available PHI

- General Department of Service Information
- Treating Physician Information
- Outcome Information

- Minimum Necessary Rule Continues to Apply

Fundraising: Opt-Out Requirements

- **Option to opt-out must be in every fundraising communication.**
  - ☑ Notice of Privacy Practices must also contain opt-out language.
- **Mechanisms for opting-out**
  - Must not be unduly burdensome or costly.
  - Look for simple, quick & inexpensive opt-out mechanisms (e.g., toll-free number and/or email address).
- **Flexibility with respect to scope of opt-out.**
  - All future fundraising communications vs. specific fundraising campaign.
  - Give the individual the option.
- **Importance of tracking individuals who have opted-out.**

Fundraising: Action Steps

- Update policy addressing the type of PHI that may be disclosed for fundraising purposes and opt-out procedures.
- Modify fundraising communications to reflect necessary opt-out language.
- Institute procedures for tracking opt-outs and opt-ins.

Access to PHI: Form & Format

- Patients have a right to access PHI maintained electronically in one or more designated record sets.
- Form & Format:
  - Of the request:
    - Form of the request at the discretion of the covered entity (written or oral).
    - Content of request at the discretion of the covered entity.
  - Of the PHI:
    - In the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed upon by the covered entity and the individual.
    - Ensure proper safeguards are in place to protect the PHI when it is disclosed in an electronic form.
- **Scope of Response to Request:** Electronic copy must contain all PHI electronically maintained in the designated record set at the time the request is fulfilled.

Access to PHI: Transmission to Third-Parties

- **If requested by an individual, a covered entity must transmit the copy of PHI directly to another person designated by the individual.**
- **Form of requests:**
  - In writing
  - Signed by the individual (including valid electronic signature)
  - Identify the designated person
  - Indicate where to send the copy of the PHI
- **Covered entity must implement reasonable safeguards to protect the information that is used or disclosed to the third-party.**

Access to PHI: Fees and Timeliness

- **Fees:**
  - **Covered entities may impose a reasonable, cost-based fee for a copy of PHI.**
  - **Reasonable, cost-base fee includes:**
    - Labor for copying PHI
    - Cost of supplies for creating paper copy or electronic media
    - Postage costs
- **Timeliness:**
  - **On-Site & Off-Site Records:** Access or a copy of the requested PHI provided within 30 days of the request.
  - **Extension:** 30-day extension available upon written notice to the requesting individual.

Access to PHI: Action Steps

- Update a policy to address individuals' right to access electronic copy of protected health information. Such policy should address:
  - Form and format
  - Scope of responses to requests.
  - Access fees.
  - Timeliness requirements.

Access to PHI: Action Steps

- Institute procedures for tracking and responding to written and/or oral access requests.
- Train workforce in access procedures.

Right to Request a Restriction of Uses and Disclosures of PHI

- Under the Final Rule, a covered entity is required to permit individuals to request restrictions on uses or disclosures of their PHI to a 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, or person on behalf of the individual other than the health plan, has paid the covered entity in full.

Restricting Disclosure of PHI

- Medical Records
  - Not necessary to create separate records or segregate PHI; Flag or make notation
- Bundled Services
  - Counsel patients on ability to unbundle and the impact
  - Individual may pay out of pocket for entire bundle

Restricting Disclosure of PHI

- Downstream Providers
  - Patient's responsibility
- HMOs
  - Contractual requirements for a provider to submit claims or disclose PHI to an HMO do not exempt the provider from obligations under the Final Rule
- Dishonored Payments
  - Make reasonable attempts to resolve payment issues
- Follow-Up Care

Restricting Disclosures of PHI: Action Steps

- Identify personnel whose job functions will be affected by the Final Rule and ensure that they are properly trained in implementing valid requested restrictions and protecting restricted PHI.
  - Consider that personnel may need training in bundled services and other aspects of the Final Rule.
- Adopt/update policies and procedures to comply with the Final Rule.
  - Document restrictions appropriately
  - Encourage counseling patients on downstream providers

Nature of Privacy Practices
Enforcement
Research
Decedents

Michael R. Callahan

Katten

Katten Muchin Rosenman LLP

Notice of Privacy Practices

- General requirement is that CEs must distribute a NPP which describes the uses and disclosures of PHI, e.g. treatment, payment and health care operations, and permitted disclosures of PHI, the CE's legal duties and privacy practices and the individual's rights relating to PHI.
- NPP must also contain a statement that any uses and disclosures other than those permitted by the Privacy Rule can only be made if the CE receives a written authorization from the individual and that the authorization may be revoked.

Notice of Privacy Practices (cont'd)

- Final rule now requires that the following statements regarding uses and disclosures of PHI requiring a prior authorization be included in NPP.
  - a statement that uses and disclosures not listed in NPP will only be made if written authorization is obtained and that it may be revoked.
  - a separate statement that if the CE intends to contact the individual to raise funds that individual has the right to opt out of receiving these communications.

Notice of Privacy Practices (cont'd)

- most uses and disclosures of psychotherapy rules require an authorization.
- uses and disclosures of PHI for marketing purposes (includes all treatment and health care operations communications where the CE receives remuneration from a third party whose product or services is being marketed require an authorization).
- For providers, NPP must inform individuals of their right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for item or service.

Notice of Privacy Practices (cont'd)

  - Must include a statement of right of affected individual to be notified of a breach of unclaimed PHI.

- If a group health plan intends to disclose a PHI for underwriting purposes, a statement that it is prohibited from using or disclosing PHI that is genetic information of an individual for such purposes must be in the NPP.

Redistribution of Revised Notices of Privacy Practices

- Health Plans
  - If health plan posts its NPP on its website then
    - Web site must prominently post the material changes re: the revised NPP by September 23, 2013 and
    - Provide the revised NPP or information about the material change and how to obtain the revised NPP in next annual mailing to individuals covered by the plan.

Redistribution of Revised Notices of Privacy Practices (Cont'd))

- If health plan does not utilize a web site it must provide the revised NPP or information about the material changes and how to receive the revised NPP to covered individuals within 60 days of the all material revisions to the NPP.
- Distributions should be provided on both paper and web-based notices.

Redistribution of Revised Notices of Privacy Practices (Cont'd)

- Health Care Providers
  - Must make revised NPP available upon request on or after effective date of revision and obtain a good faith acknowledgment of receipt form.
  - Must have revised NPP available at heath care delivery site.
  - Must post revised NPP in a clear and prominent location (can also post a summary and make full NPP available)

Redistribution of Revised Notices of Privacy Practices (Cont'd)

- Need not print and hand out revised NPP to all seeking treatment.
- Can be distributed by email if individual has agreed to receive an electronic copy.

NPP Action Steps

- Providers and health plans will need to revise and redistribute NPPs.

Enforcement Rule - Categories of Violations and Respective Penalty Amounts

Violation Category	Each Violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100-$50,000	$1,500,000
(B) Reasonable Cause	$1,000–$50,000	$1,500,000
(C)(i) Willful Neglect-Corrected	$10,000–$50,000	$1,500,000
(C)(ii) Willful Neglect-Not Corrected	$50,000	$1,500,000

Enforcement Rule - Categories of Violations and Respective Penalty Amounts

- Keep in mind that the $1.5 million yearly limitation is based on a per covered entity/business associate and a per requirement basis and therefore total penalties can exceed $1.5 million.

Enforcement Rule – Civil Monetary Penalties

- There are four different levels of penalties depending on increasing culpability based on the nature of the conduct involved and application of the definitions of "reasonable cause", "reasonable diligence" and "willful neglect".
  - Reasonable Cause
    - An act or omission in which a covered entity or business associate knew or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision but in which the covered entity did not act with willful neglect.

Enforcement Rule – Civil Monetary Penalties

Example:

- Covered entity fails to timely respond to an individual request for access to records even though it had appropriate policies and procedures only because the volume of requests made it unable to respond to all requests despite good faith efforts to do so. Covered entity responded as soon as it could.
- Different outcome if covered entity did not have policies or did not attempt to clear up backlog, did not provide explanation for the delay or when request would be honored.

Enforcement Rule – Civil Monetary Penalties

- Knowledge and Reasonable Diligence
  - The knowledge involved must be knowledge that a violation occurred, not just knowledge of the facts constituting the violation.

  Example:

    - Covered entity inadvertently gave patients an incomplete notice of privacy practice because of a printing error. Covered entity had an otherwise compliant NPD and associated policies and training, a small number of patients were affected and error was isolated and corrected.

Enforcement Rule – Civil Monetary Penalties

- Willful Neglect
  - Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

  Examples:

    - Covered entity disposes of several hard drives with electronic PHI in an unsecured dumpster. Covered entity has no policies on how to effectively dispose of PHI.

Enforcement Rule – Civil Monetary Penalties

- Covered entity employee loses a laptop with unencrypted PHI and purposefully decided not to provide required notification.

Enforcement Rule – Willful Neglect

- Noncompliance Due to Willful Neglect
  - Under Final Rule, Secretary will investigate, as opposed to may investigate, any complaint when a preliminary review of the facts indicates a possible violation due to willful neglect.
  - Secretary still has discretion to investigate other complaints.
  - Secretary may also conduct a compliance review when a preliminary review indicates a possible violation due to

Enforcement Rule – Willful Neglect

willful neglect although usually conducted when there are alleged violations brought to Department's attention through some means other than a complaint.

- Proposed language which provided that the Secretary will attempt to resolve investigations and compliance reviews by information means has been changed to "may" attempt. In reaction to a finding of willful neglect so as to allow for the immediate imposition of a civil penalty.
- Secretary still has authority to resolve informally where appropriate.

Enforcement Rule – Willful Neglect

- Secretary has authority, however, to move directly to a civil monetary penalty without first exhausting informal resolution efforts.
  - Keep in mind that information/evidence of violation and PHI can be shared with other enforcement agencies.

Enforcement Rule - Factors in Determining Amount of Civil Penalties

- The nature and extent of the violation, consideration of which may include but is not limited to:
  - The number of individuals affected; and
  - The time period during which the violation occurred.
- The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:
  - Whether the violation caused physical harm;

Enforcement Rule - Factors in Determining Amount of Civil Penalties (cont'd)

- Whether the violation resulted in financial harm;
- Whether the violation resulted in harm to an individual's reputation; and
- Whether the violation hindered an individual's ability to obtain health care.

- The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

Enforcement Rule - Factors in Determining Amount of Civil Penalties (cont'd)

- Whether the current violation is the same or similar to previous indications of noncompliance;
- Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;
- How the covered entity or business associate has responded to technical assistance from the Secretary provided in the contest of a compliance effort; and
- How the covered entity or business associate has responded to prior complaints.

Enforcement Rule - Factors in Determining Amount of Civil Penalties (cont'd)

- The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:
  - Whether the covered entity or business associate had financial difficulties that affected its ability to comply;
  - Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

Enforcement Rule - Factors in Determining Amount of Civil Penalties (cont'd)

- The size of the covered entity or business associate.

- Such other matters as justice may require.

Enforcement Rule - Affirmative Defenses

- Prior to February 18, 2011 a CMP cannot be imposed if criminally punishable.
- If criminal penalties are imposed.
- If violation occurred prior to February 18, 2009, CMP cannot be imposed
  - if CE (or its agent) did not have knowledge of the violation and by exercising reasonable diligence would not have known a violation occurred

Enforcement Rule - Affirmative Defenses

- or circumstances made it unreasonable for the CE to comply, despite exercise of ordinary care and prudence.
  - If not found to be willful neglect.
  - AND either corrected within 30 days after it knew or should have known a violation occurred .

Enforcement Rule - Affirmative Defenses

- Enforcement Rule Action Steps
  - See attached description of OCR enforcement statistics and actions
  - Conduct gap analysis.

Research

Compound Authorizations

- Privacy Rule generally prohibits conditioning of treatment, payment or enrollment in a health plan or benefits eligibility on signing an authorization allowing for disclosure of PHI other than for TPO purposes.
- One exception is that an authorization can be required if treatment is related to research purposes such as a clinical trial.

Research (cont'd)

- Under prior provisions, "compound authorizations" which allowed for identified disclosure of PHI could not be combined with any other legal permission which granted an unconditional authorization.
- In response to comments and concerns and in order to make these provisions more consistent with Common Rule practices, conditioned and unconditional research authorizations can be combined if:
  - Form clearly differentials between the conditioned and unconditioned research component.

Research (cont'd)

- Form clearly allows the individual the option to opt in to any unconditioned research activity except research involving use or disclosure of psychotherapy notes.
  - Allowing individual with only the option to opt out is not permitted.
- Must still comply with the form and content requirements for authorization forms.
- Covered entities have flexibility on what method to utilize in order to distinguish between continued and

Research (cont'd)

- unconditional research projects and how to opt in to unconditional portion.
  - Examples:
    - Opt in check box
    - Separate signature for unconditional opt in portion
    - Separate page describing unconditional research portion
    - Combination of all of the above

Future Research

- In an effort to align with Common Rule practices with respect to obtaining informed consent, the described "purpose" of research provisions in authorization form no longer requires the purpose to be study specific.
- Authorization form, however, must adequately describe such purposes so that an individual would reasonably conclude that PHI could be used or disclosed for future research.

Research (cont'd)

- Examples:
  - A specific statement or explanation of future contemplated research projects
  - Generalized statement as to possible projects.
  - Identification that future medical records could be used for research
- Description of PHI to be used can reference information collected beyond the time of the original study.
- Privacy Rule authorization rules allows PHI to also be disclosed to a "class of persons who will or may be conducting research".

Research (Cont'd)

- Research Action Steps
  - CEs conducting research now have the option to combine authorization forms to contain a single authorization for conditional and unconditional research projects using PHI.
  - Similarly, authorization forms can be combined to identify specific research projects and future unspecified projects.
  - Revise policies accordingly.

Decedent Information

- Privacy Rule protection expires 50 years after death – information is no longer treated as PHI.
- Must still comply with more restrictive state laws on disclosures.
- CEs have the option of extending the protection beyond 50 years where sensitive information is involved, i.e., HIV/AIDs, substance abuse, mental illness.
- 50 year requirement is not a record retention requirement.

Decedent Information(cont'd)

Disclosures to Decedent's Family Members and Others Involved in Care

- Such disclosures permitted unless inconsistent with decedent's prior expressed preferences prior to death.
- Disclosure limited to PHI relevant to person's involvement in health care or for payment.
- Should not share PHI about past or unrelated medical problems.

Decedent Information - Disclosures

- Disclosures are permissive and not required.
- Disclosures, depending on the circumstances, can include spouses, parents, children, domestic partners, other relatives or friends, personal representative, executor or trustee.
- No set burden of proof of establishing relationship to decedent.

Decedent Information (cont'd)

- Decedent Action Steps
  - Decide whether CE wishes to abide by more flexible standards.
  - Revise policies accordingly.

Katten
Katten Muchin Rosenman LLP

Katten Muchin Rosenman LLP Locations

AUSTIN
One Congress Plaza
111 Congress Avenue
Suite 400
Austin, Texas 78701
512.650.1000 tel
512.650.1002 fax

CHICAGO
525 W. Monroe Street
Chicago, IL 60661-3693
312.902.5200 tel
312.902.1061 fax

LOS ANGELES
515 South Flower Street
Suite 1000
Los Angeles, CA 90071-2212
213.788.7445 tel
213.788.7380 fax

ORANGE COUNTY
650 Town Center Drive
Suite 700
Costa Mesa, CA 92626-7122
714.386.5708 tel
714.386.5736 fax

CENTURY CITY
2029 Century Park East,
Suite 2600
Los Angeles, CA 90067-3012
310.788.4400 tel
310.788.4471 fax

IRVING
5215 N. O'Connor Boulevard,
Suite 200
Irving, TX 75039-3732
972.868.9058 tel
972.868.9068 fax

NEW YORK
575 Madison Avenue
New York, NY 10022-2585
212.940.8800 tel
212.940.8776 fax

SHANGHAI
Ste. 4906 Wheelock Square
1717 Nanjing Road West
Shanghai 200040
China
011.86.21.6039.3288 tel
011.86.21.6039.3223 fax

CHARLOTTE
550 South Tryon Street,
Suite 2900
Charlotte, NC 28202-4213
704.444.2000 tel
704.444.2050 fax

LONDON
125 Old Broad Street
London EC2N 1AR
+44.20.7776.7620 tel
+44.20.7776.7621 fax

OAKLAND
1999 Harrison Street, Suite 1800
Oakland, CA 94612-0850
415.360.5444 tel
415.704.3151 fax

WASHINGTON, D.C.
2900 K. Street,
North Tower - Suite 200
Washington, DC 20007-5118
202.625.3500 tel
202.298.7570 fax

www.kattenlaw.com