Training Update for HIPAA Compliance Administrators

HIPAA Omnibus Final Rule Modifications
This presentation is intended as an overview of the HIPAA Privacy Final Rule by a subject matter expert who is a non-lawyer.

This presentation covers a selected group of the most important Final Rule modifications that impact the greatest number of CEs and BAs.

Some of the Omnibus Final Rule changes are quite straightforward; but others, especially marketing, fundraising and research are more complex.

Be sure to consider utilizing legal counsel if you are embarking upon a marketing, fundraising or research project (unless expertise lays within the IRB or other controlling group).
If your organization has consistently kept up with the privacy rules changes since HITECH in 2009, the new Omnibus Final Rule modifications will not be overly complex. It’s likely you have already implemented most of the rules now in effect since most of the proposed and interim rules were adopted without changes. If not, begin work to get into compliance by September 23, 2013.
Section 1:

Summary of Modifications to HIPAA Rules
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/00</td>
<td>The First HIPAA Privacy Final Rule; 45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule</td>
</tr>
<tr>
<td>8/02</td>
<td>Modification to HIPAA Privacy Rules; Final Rule 45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule</td>
</tr>
<tr>
<td>2/09</td>
<td>ARRA ‘American Recovery and Reinvestment Act Subtitle D (HITECH Act)</td>
</tr>
<tr>
<td>7/09</td>
<td>Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Notice of Proposed Rulemaking</td>
</tr>
<tr>
<td>8/09</td>
<td>Breach Notification for Unsecured Protected Health Information; Interim Final Rule</td>
</tr>
<tr>
<td>8/09</td>
<td>FTC Breach Rule for Personal Health Records; Final Rule</td>
</tr>
<tr>
<td>10/09</td>
<td>HIPAA Administrative Simplification; Enforcement; Interim Final Rule</td>
</tr>
<tr>
<td>7/10</td>
<td>Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule</td>
</tr>
<tr>
<td>5/11</td>
<td>HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act; Notice Proposed Rulemaking</td>
</tr>
<tr>
<td>11/12</td>
<td>Guidance Related to De-identification of PHI; OCR Website Guidance</td>
</tr>
<tr>
<td>01/13</td>
<td>Omnibus Privacy (and Security) Final Rule Modifications</td>
</tr>
</tbody>
</table>
Omnibus Final Rule:

- Increases liability and focus on privacy and security compliance for Business Associates (BAs) and upon Covered Entities (CEs) to administer and monitor their BAs. BAs have the same duties for their sub-contractors.
- Strengthens the position that individual authorizations are required for marketing, fundraising and selling PHI activities.
- Strengthens patient rights to receive electronic copies of their health information. Requires a compressed time frame for delivery to patient (30 days plus one 30 day extension).
- Clarifies access and disclosure of healthcare records containing PHI.
- Reaffirms restriction requests for health plans on treatment paid out-of-pocket.
- Requires material changes to NPP (Notice of Privacy Practices); NPP distribution (re-distribution required for health plans, not providers).
Omnibus Final Rule:

- **Adopts previous HITECH enforcement rules and strengthens willful neglect compliance enforcement.**

- Formally adopts the 4-tiered penalty structure from previous rules.

- **Changes the breach notification framework** for Breach Notification for Unsecured Protected Health Information from a ‘potential harm to individual threshold’ standard to a ‘low probability of compromise’ standard.

- **Clarifies that health plans cannot use genetic information for underwriting.** Does not impact provider use of genetic information for treatment purposes.

- **Allows compound authorizations** for conditioned and unconditioned research.

- **Allows disclosure of PHI to schools for immunization data,** with only verbal approval.
Section 2:

Important Rule Changes
• Business Associates (BAs) are now directly liable for breach and may sometimes have to report them.

• The Omnibus Privacy Final Rule added language to the definition of ‘breach’ to clarify that an impermissible use or disclosure of protected health information is presumed to be a breach unless the CE or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

  – To further ensure that this provision is applied uniformly and objectively by CEs and BAs, we have removed the harm standard and modified the risk assessment to focus more objectively on the risk that the PHI has been compromised.

• A bright-line standard is not used to determine a breach. This is important as it cuts down on the number of reportable breaches as opposed to just having to report all incidents involving impermissible access, use or disclosure.

• The ‘Breach Safe Harbor’ through the use of encryption is maintained.
To demonstrate that there is a low probability that PHI has been compromised, a CE or BA must perform a risk assessment that addresses, at a minimum, the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.
The first factor requires CEs and BAs to evaluate the nature and the extent of the PHI involved, including the types of identifiers and the likelihood of re-identification of the information.

- To assess this factor, entities should consider the type of PHI involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature.

  - For example, with respect to financial information, this includes credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud.
  
  - With respect to clinical information, this may involve considering not only the nature of the services or other information but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results).
  
  - Considering the type of PHI involved in the impermissible use or disclosure will help entities determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient’s own interests.
  
  - Additionally, in situations where there are few, if any, direct identifiers in the information impermissibly used or disclosed, entities should determine whether there is a likelihood that the PHI released could be re-identified based on the context and the ability to link the information with other available information.
The 2nd factor requires CEs and BAs to consider the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made.

- Entities should consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information; there may be a lower probability that the PHI has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity.

- We also emphasize that this factor should be considered in combination with the factor discussed previously regarding the risk of re-identification.

- If the information impermissibly used or disclosed is not immediately identifiable, entities should determine whether the unauthorized person who received the PHI has the ability to re-identify the information.
The 3rd factor requires CEs and BAs to investigate an impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed.

- For example, as discussed in the interim final rule, if a laptop computer was stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed.

- In contrast, however, if a CE mailed information to the wrong individual who opened the envelope and called the entity to say that she received the information in error, then, in this case, the unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error.
The 4th and final factor in the Final Rule requires CEs and BAs to consider the extent to which the risk to the PHI has been mitigated. CEs and BAs should attempt to mitigate the risks to the PHI following any impermissible use or disclosure, such as by obtaining the recipient’s satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.

- We note that this factor, when considered in combination with the factor regarding the unauthorized recipient of the information discussed previously, may lead to different results in terms of the risk to the PHI.

- For example, a covered entity may be able to obtain and rely on the assurances of an employee, affiliated entity, BA, or another CE that the entity or person destroyed information it received in error, while such assurances from certain third parties may not be sufficient.
The fact that information only is impermissibly used within a CE or BA and the impermissible use does not result in further impermissible disclosure outside the entity, is something that may be taken into account in conducting the risk assessment and may reduce the probability that the PHI has been compromised.

Other factors may also be considered where necessary.

HHS/OCR expects these risk assessments to be thorough, completed in good faith, and for the conclusions reached to be reasonable. If an evaluation of the factors discussed above fails to demonstrate that there is a low probability that the protected health information has been compromised, Breach Notification is required.

We do note, however, that a CE or BA has the discretion to provide the required notifications following an impermissible use or disclosure of protected health information without performing a risk assessment.

Because the final rule clarifies the presumption that a breach has occurred following every impermissible use or disclosure of protected health information, entities may decide to notify without evaluation of the probability that the protected health information has been compromised.

In the future, we will issue additional guidance to aid CEs and BAs in performing risk assessments with respect to frequently occurring scenarios.

HHS/OCR has removed the exception for limited data sets that do not contain any dates of birth and zip codes.
BA Breach determination and notification requirements were modified, adding to the BAs responsibilities.

- Final Rule directly says that BAs must have contracts or other arrangements in place to provide satisfactory assurances that they will appropriately safeguard the ePHI they create, receive, maintain or transmit on behalf of the CE.

  - This means BA Privacy and Security questionnaires are critical and will dramatically increase under this rule.

- Omnibus Rule provides that there must be an agreement between the business associate and its subcontractor that provides that the subcontractor is subject to the same HIPAA requirements for access and use of PHI as the business associate. Business associates’ subcontractors are now contractually obligated to comply with certain HIPAA requirements, but not directly subject to HHS enforcement authority.
• Business Associates now include:
  – PSOs (Patient Safety Organizations)
  – HIOs (HIE, RHIO)
  – E-prescribing gateways
  – PHR vendors that provide services on behalf of a CE

• BA is directly liable under the Privacy Rule for uses and disclosures of PHI that are not in accord with its business associate agreement (BAA) or the Privacy Rule.

• BA is directly liable for providing information to OCR for investigations and notifying CEs of potential violations.
• BAs directly liable for failing to utilize Minimum Necessary.

• BAs are directly liable under HIPAA for the following:
  – Wrongful (impermissible) access, use or disclosures
  – Failure to provide access to a copy of ePHI to either the CE, the individual or the individual’s designee as specified in the BAA
  – Failure to provide AOD (Accounting of Disclosures)
  – Failure to provide breach notification to a CE
  – Failure to comply with all applicable HIPAA Privacy and Security Rules

• HHS has emphasized the importance of business associate contracts (i.e. BAA)
Enforcement

• The Final Rule requires Office for Civil Rights (OCR) to formally investigate a complaint if a preliminary investigation of the facts of the complaint indicates a possible, not probable, violation due to willful neglect and to impose a civil money penalty for a violation due to willful neglect.
  – In general Omnibus strengthens enforcement, especially in regards to willful neglect by adopting previously issued privacy and security rules.

• The tiered penalty structure remains in place.

• ‘Willful neglect’ determinations for enforcement purposes is founded upon evidence from OCR’s investigation of the allegations.

• The Burden of Proof in providing documentation to support actions is placed upon the CE and BA in many places within the rules.
• The factors OCR general factors they consider in determining a CMP (Civil Monetary Penalty).
  – The nature and extent of the violation.
  
  • Time period during which the violation(s) occurred and the number of individuals affected.
  • The nature and extent of the harm resulting from the violation.
  • The history of prior compliance with HIPAA (administrative simplification), including violations by the covered entity or business associate.
  • The financial condition of the covered entity or business associate.
  • Such other matters as justice may require.

• The facts of the situation will determine whether reputational harm has occurred, such as whether the unlawful disclosure resulted in adverse effects on employment, standing in the community, or personal relationships.
• **OCR currently conducts a preliminary review of every complaint received** and proceeds with the investigation in every eligible case where its preliminary review of the facts indicates a possible violation of the HIPAA Rules.

  – OCR will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.

    • OCR has continued discretion with respect to investigating any other complaints.

    • OCR may on a case-by-case basis expand the preliminary review and conduct additional inquiries for purposes of identifying a possible violation due to willful neglect.

  – OCR generally conducts Compliance Reviews to investigate allegations of violations of the HIPAA Rules brought to their attention through a mechanism other than a complaint.

  – Complaints or Compliance Reviews can be the basis of an investigation.
These are material changes, but the rules about distribution of the NPP remain unchanged, including:

- When a health care provider with a direct treatment relationship with an individual revises the NPP, the health care provider must make the NPP available upon request on or after the effective date of the revision and must have the NPP available at the delivery site and to post the notice in a clear and prominent location.

- Providers are not required to print and hand out a revised NPP to all individuals seeking treatment.

- Providers must post the revised NPP in a clear and prominent location and have copies of the NPP at the delivery site for individuals to request to take with them.
• Providers are only required to give a copy of the NPP to, and obtain a good faith acknowledgment of receipt from new patients.

• OCR clarifies that while health care providers are required to post the NPP in a clear and prominent location at the delivery site, providers may post a summary of the notice in such a location as long as the full notice is immediately available (such as on a table directly under the posted summary) for individuals to pick up without any additional burden on their part.
  – It would not be appropriate, however, to require the individual to have to ask the receptionist for a copy of the full NPP.

• If a provider has already revised their NPP and its fully compliant they are not required to reprint or re-distribute.

• Health plans do have to distribute the revised NPP to their members; there are rules for allowing them over a year to do so.
NPP updates must include (if applicable by service delivery):

1. Inform individuals of their new right to restrict certain disclosures of protected health information to a health plan where the individual pays out of pocket in full for the health care item or service.

2. A statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of protected health information for marketing purposes, and disclosures that constitute a sale of protected health information require authorization.

3. A statement that other uses and disclosures not described in the NPP will be made only with authorization from the individual.

4. A statement in the NPP regarding fundraising communications and an individual’s right to opt out of receiving such communications, if a CE intends to contact an individual to raise funds for the CE.

5. A statement about breach notification.
• Definition of ‘sale of PHI’ is revised to generally mean ‘a disclosure of PHI by a CE or BA, if applicable, where the CE or BA directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.’

  – A sale of PHI occurs when the CE or BA primarily is being compensated to supply data it maintains in its role as a CE or BA.

• Such disclosures require the individual’s authorization unless they otherwise fall within an exception.
Commenters asked that the Final Rule clarify that business associates can continue to receive payment of costs from third parties (i.e. Release of Information vendors) for providing this service on behalf of covered entities.

- The Final Rule permits the same types of costs under this exception as the research exception, as well as costs that are in compliance with a fee schedule provided by State law or otherwise expressly permitted by other applicable law.

- Thus, costs may include the direct and indirect costs to prepare and transmit the data, including labor, materials, and supplies, but not a profit margin.

OCR intends to continue to work with interested stakeholders to develop more guidance on direct and indirect costs and on remuneration.
This section also specifies two circumstances in which authorization from the individual must be obtained:

- (1) Most uses and disclosures of psychotherapy notes; and

- (2) Uses and disclosures for marketing purposes.
**Fundraising**

- Final Rule expands the type of information that can be used for fundraising without patient authorization to include the department of service information, the identity of the treating physician, and health insurance status.

- The Final rule does not modify the types of communications that are currently considered to be for fundraising purposes.

  - A communication to an individual that is made by a covered entity, an institutionally related foundation, or a business associate on behalf of the covered entity for the purpose of raising funds for the covered entity is a fundraising communication.

- Privacy Rule has always required that such communications contain a description of how the individual may opt out of receiving further fundraising communications.
Marketing

• The final rule significantly modifies the proposed rule's approach to marketing by requiring authorization for all treatment and health care operations communications where the covered entity receives financial remuneration for making the communications from a third party whose product or service is being marketed.
  
  – A device manufacturer cannot pay for marketing of that device to patients without their authorization.

• Under the final rule, for marketing communications that involve financial remuneration, the CE must obtain a valid authorization from the individual before using or disclosing protected health information for such purposes, and such authorization must disclose the fact that the CE is receiving financial remuneration from a third party.

• There continues to be a stand-alone exception for prescription refill reminders and certain drugs and biologics.
  
  – Be careful how these are implemented and be sure to track the CEs or physicians ‘reasonable costs’.
The Final Rule amends the Privacy Rule to require that if an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets, the CE must provide the individual with access to the electronic information 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 to by the CE and the individual.
– In such cases, to the extent possible, we expect covered entities to provide the individual with a machine-readable copy of the individual’s PHI.

The Department considers machine-readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer.

For example, this would include providing the individual with an electronic copy of the PHI in the format of MS Word or Excel, text, HTML, or text-based PDF, among other formats. PDF is recognized as a acceptable electronic format, although OCR remains technically neutral.

If an individual requests a form of electronic copy that the CE is unable to produce, the CE must offer other electronic formats that are available if the individual declines to accept any of the electronic formats that are readily producible by the CE, the CE must provide a hard copy as an option to fulfill the access request.
How and to what extent a BA is to support or fulfill a CEs obligation to provide individuals with electronic access to their records will be governed by the BAA between the CE and the BA.

Electronic documents to qualify as written documents.

Electronic signatures to satisfy any requirements for a signature, to the extent the signature is valid under applicable law.

If the CE chooses to require a written request, it has flexibility in determining what information to put into the request form as long as the request form is not in any way designed to discourage an individual from exercising his or her right.

CEs are not required to scan paper documents to provide electronic copies of records maintained in hard copy.

– OCR notes that for CEs that have mixed media, it may in some cases be easier to scan and provide all records in electronic form rather than provide a combination of electronic and hard copies, however this is in no way required.

– Therefore scanned copies can be considered electronic.
Access by Individuals to PHI

- OCR recognizes what is available in a readable electronic form and format will vary by system and that CEs will continue to improve their technological capabilities over time.

- CEs are allowed the flexibility to provide readily producible electronic copies of PHI that are currently available on their various systems.

- A CE is not required to purchase new software or systems in order to accommodate an electronic copy request for a specific form that is not readily producible by the CE at the time of the request, provided that the covered entity is able to provide some form of electronic copy.

- OCR notes that some legacy or other systems may not be capable of providing any form of electronic copy at present and anticipate that some CEs may need to make some investment in order to meet the basic requirement to provide some form of electronic copy.
• It may not be appropriate for CEs (or BAs) to accept the use of external portable media on their systems.

  – CEs (and BAs) are required by the Security Rule to perform a risk analysis related to the potential use of external portable media, and are not required to accept the external media if they determine there is an unacceptable level of risk.

  – However, CEs are not then permitted to require individuals to purchase a portable media device from the covered entity if the individual does not wish to do so.

    • The individual may in such cases opt to receive an alternative form of the electronic copy of the protected health information, such as through email.

      – CEs are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email.

• The Final Rule modifies the timeliness requirements for right to access and to obtain a copy of PHI to 30 days from the date of the request.

  – A 30 day extension can be invoked, once per request, so the total for response to a request for access or copies changes from 60 day + 30 day extension to 30 days + 30 day extension, from 90 days total to 60 days total.
Right to Restrictions

• Basically, previous rule making had outlined the right of restriction rules and Omnibus adopted them.

• If you were proactive in creating new polices, NPP and procedures for these types of restrictions you should be ready now.

• Some parties decided to wait to update their NPPs and implement the new restriction requirements until the Final Rule was published. Now’s the time to start those revisions and update your NPP, policies and procedures.

• Setting flags to remind workforce members (and BAs if appropriate) that required or agreed upon restrictions are in place is not always easy. Develop a process or leverage technology to help with this challenge.
Right to Restrict

- Patients have the right to request additional restrictions to the use and disclosure of their health information; your organization may not have to abide by these restrictions.

- **There is a restriction which your organization has to abide by**—a request for restriction on use or disclosure of PHI related to health plans for services or items that they have paid out of pocket and have a current $0 balance; for payment and operations purposes only.

- If /when you do have to provide a restriction to PHI use and disclosure, be sure to work out processes and flags in your systems to call out the request.

- Be aware that agreeing to a restriction means you have to manage it, this can be very difficult as most EHR type systems don’t have a way to tack them.

- No healthcare provider should ever restrict the use of PHI for treatment purposes.

- Be aware of strict timeframes (typically 60 days) for responses to these requests.

- Individuals who wish to request a restriction should be referred to the Health Information Management or other appropriate department or staff.

- All communications and documentation associated with these requests must be kept for the entire 6-year HIPAA retention period.
• The Security Rule modifications are mostly for alignment and harmonization with the Privacy Rule.

• Direct liability for compliance with the Security Rule to business associates.

• BAs and Sub-contractors are required to have in place security practices for security rule compliance.

• Sub-contractor second tier has potential breach they notify BA subcontractor who notifies the CE, up the chain.

• There exists flexibility for organizations to scale their security practices, which is not to say that some do not have to be met. But the scale of how they are met, given options, can vary.

  — In deciding which security measures to use, a covered entity or business associate should take into account its size, capabilities, the costs of the specific security measures, and the operational impact. The costs of implementing the Security Rule for large, mid-sized, or small business associates will be different.
**Definition of Electronic Media**

- Confirms copier, fax and similar device based info can be PHI that must appropriately protected and secured, by monitoring or restricted access and appropriate safeguards applied when turned-in or sold.

**Definition of Protected Health Information**

- PHI ceases to be PHI, with no application of privacy and security rules 50 years after death of the individual to whom the PHI relates.

- The final rule adopts the proposal to amend § 164.510(b) to permit covered entities to disclose a decedent’s PHI to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the CE (or BA).
Disclosure of Student Immunizations to Schools

• The privacy rule now permits a CE to disclose proof of immunization to a school where State or other law requires the school to have such information prior to admitting the student.

• Written authorization will no longer be required to permit this disclosure; CEs will still be required to obtain agreement, which may be oral, from a parent, guardian or other person acting in loco parentis for the individual, or from the individual himself or herself, if the individual is an adult or emancipated minor.

  – The final rule additionally requires that CEs document the agreement obtained under this provision.
• The Final Rule protects Genetic Information; applies to health plans of all types.
  – Except long term care plans.

• Restricts the use of genetic tests or other genetic information for underwriting purposes.

• Differentiates genetic information for manifested diseases.

• Does not affect access, use or disclosure by providers.

• Genetic Information may not rise to the level of ‘super-confidential’; but, you should be careful with its disclosure.
Section 3:

Top 10 tasks for Omnibus Compliance
Covered Entitles (CEs), Business Associates (BAs) and Their Sub-Contractors need to address the following tasks in order to become compliant with the Omnibus Final Rule modifications by September 23, 2013.

1. Perform a HIPAA Omnibus Rule modification assessment of your privacy and security compliance programs for compliance with the new rules to determine a gap checklist.

   - This assessment should be a part of your on-going, dynamic compliance program evaluation.
   - Periodic privacy and security risk assessments are recommended and performing them should be considered while updating to the new rules.
     * Fully document this assessment and be able to produce it if investigated, reviewed or audited.
     * What policies, procedures (workflows) and forms need to be created or updated?

2. Evaluate Business Associates and inquire as to their Sub-contractor’s privacy and security compliance programs.

   * Entities that do not have privacy and security compliance programs will need to create one.
3. Review your business process workflows and staffing requirements for your complete privacy and security compliance operations and deep, well-indexed documentation.

Important workflows to evaluate include:

– Patient access to their PHI. Remember MU requirements too.
– Other patient’s rights, i.e. restriction and amendment requests.
– Breach determination and notification with the new ‘low possibility of compromise’ standard.

4. Evaluate options for automation of your compliance documentation processes.

• The Omnibus Rule calls for consistency and uniformity in breach determination.
• The OCR audits call for in-depth documentation.
• All of these requirements raise the bar on your documentation practices
5. Update, post and implement your new Notice of Privacy Practices.
   • Distribute, if a health plan

6. Modify Business Associate Agreement (BAA) (or if a BA, your Sub-Contractor’s boilerplate).
   • Engage business associates (or sub-contractors) with established BAAs to address issues needed for Omnibus Final Rule compliance.
   • CEs: Assess your business associates for privacy and security compliance.
   • BAs: Assess your sub-contractors.
     » Utilize a uniform assessment/approach when evaluating
     » Set up an ongoing monitoring program for CEs to BA and BA to Sub-contractor assessment

Work to ensure your entire chain of PHI management is breach compliant.
7. Constantly work to increase the amount of ‘secured PHI’ through encryption in order to have as much PHI within the Breach Safe Harbor, as possible.

8. Continue to strengthen safeguards and refine policies for mobile devices, cloud computing and other areas of significant growth and technological change.

9. Become pro-active in breach (wrongful access, use or disclosure) detection and prevention with the implementation of regular auditing and monitoring.
   
   • Review your Designated Record Set audit logs and reports to determine how to perform routine audits for inappropriate access, use or disclosure.
   
   • Automate audit log monitoring with software to the extent you can.

10. Update your educational materials and train your workforce on the new rules, along with existing training programs.
Conclusion

• The Final Rule’s effective date is March 26, 2013

• The deadline for implementation is September 23, 2013—this is the day implementation is required.

• You can continue to perform breach risk analysis under interim final rule until September 23, 2013.

Recommendation for Handling Breach Determination
Keep managing privacy compliance as you have been under current (interim) rules. Begin using the new Breach analysis approach on September 23, 2013.

• Always perform and maintain consistent documentation—it may be called for in an investigation or audit. Keep all documentation at least 6 years.

• If you are a larger facility, be sure to evaluate your privacy management automation.
Omnibus Final Rule as published in the Federal Register on January 25, 2013