ALSTON & BIRD LLP

WWW.ALSTON.COM

FEBRUARY 1, 2013

HIPAA/HITECH Act Omnibus Rule Checklist

This checklist is a tool to assist covered entities, business associates and subcontractor business associates to plan their implementation of the January 25, 2013, HIPAA/HITECH Act Omnibus Rule, which significantly amended the HIPAA/HITECH Act Privacy, Security, Breach Notification, and Enforcement Rules.[1] This checklist is intended to guide discussions regarding needed updates and revisions; additional topics and requirements may apply in specific situations. This checklist was prepared by Angela Burnette, Paula Stannard and Dawnmarie Matlock. If you have any questions or if we can assist with any of these tasks, please contact Angela, Paula, Dawnmarie or your Alston & Bird attorney.[2]

If you are a Covered Entity:

- ☐ Review and revise your Notice of Privacy Practices (NPP) to include numerous statements now required by the Omnibus Rule.
- ☐ Consider and confirm how these "material changes" to your NPP will be distributed, as required by the Omnibus Rule.
- ☐ Review the revised definition of "marketing." Determine whether and to what extent protected health information (PHI) is used by your organization for marketing. Does an exception apply? If an authorization is required, develop or update your authorization form.
- ☐ Review the new definition of "sale" of PHI. Determine whether your organization's use or disclosure of PHI would fall within the definition of a "sale" of PHI. If so, does an exception apply? If no exception applies, develop new authorization to permit such uses of PHI.
- ☐ Review and update your existing HIPAA authorization form.
- ☐ Revise your form Business Associate Agreement to include new provisions required under the Omnibus Rule.
- ☐ Prepare an amendment for Business Associate Agreements already signed to add new provisions required under the Omnibus Rule.

---

1 We discussed these significant changes in the Alston & Bird advisory "Overview of HIPAA/HITECH Act Omnibus Final Rule" issued on January 25, 2013, which accompanies this checklist and is also available at http://www.alston.com/publications/.

2 Angela Burnette, 404.881.7665, angie.burnette@alston.com; Paula Stannard, 202.239.3626, paula.stannard@alston.com; Dawnmarie Matlock, 404.881.4253, dawnmarie.matlock@alston.com.

- ☐ Review and update, as necessary, your HIPAA Privacy policies and procedures, including the definition of PHI (includes genetic information), access to records (can include PHI maintained electronically even if not an electronic medical record), requested disclosures to third parties, requested restrictions, marketing, fundraising, notification to persons involved in patient's care, research, decedents and immunization records.
- ☐ Revise breach notification policies and procedures in light of the new definition of breach and the new requirements and procedures for performing a risk assessment.
- ☐ Review your research activities; consider whether to develop and use compound authorizations and whether to include authorization for future research.
- ☐ Review whether any research activities involve psychotherapy notes. Authorization for use or disclosure involving psychotherapy notes can only be combined with another authorization relating to psychotherapy notes.
- ☐ Review and update methods and data management systems for your entity's fundraising communications, including requirements related to persons opting out of receiving such communications, methods to track persons who opt out and methods to track persons opting back in.
- ☐ Review and update the type of demographic and other information covered entities are now permitted to use as part of fundraising communications.
- ☐ Review your entity's desired use of decedents' PHI in light of the new 50-year provision.
- ☐ Update HIPAA and breach notification training.
- ☐ In light of changes to the Enforcement Rule, consider whether you need to develop and implement policies and procedures for monitoring business associate compliance with HIPAA.
- ☐ If you are a health plan, there are new Privacy Rule provisions regarding genetic information that may require changes to your Notice of Privacy Practices and restrictions on your use of genetic information.
- ☐ If you are a "Hybrid Covered Entity," review the level at which contracting and other organizational matters are conducted.

If you are a Business Associate (BA):

- ☐ Revise your form BA Agreement to include new provisions required under the Omnibus Rule.
- ☐ Revise your form Subcontractor BA Agreement to include new provisions required under the Omnibus Rule.
- ☐ Review BA Agreements already signed and prepare an amendment to include new provisions required under the Omnibus Rule.
- ☐ Review Subcontractor BA Agreements already signed and prepare an amendment to include new provisions required under the Omnibus Rule.
- ☐ Develop or revise HIPAA Privacy policies and procedures, including HIPAA rules newly applicable to BAs.
- ☐ Develop or revise HIPAA Security policies and procedures, including HIPAA rules newly applicable to BAs.
- ☐ Revise breach notification policies and procedures in light of the new definition of breach and the new requirements and procedures for performing a risk assessment.
- ☐ Update HIPAA and breach notification training.

If you are a Subcontractor Business Associate (Sub BA):

- ☐ Confirm whether you meet the definition of a Sub BA; if so, you are now included in the definition of a Business Associate unless another exception applies.
- ☐ Revise your form Sub BA Agreement to include new provisions required under the Omnibus Rule.
- ☐ Consider whether to amend Sub BA Agreements already signed.
- ☐ Develop or update HIPAA Privacy policies and procedures to include new requirements under the Omnibus Rule.
- ☐ Develop or update HIPAA Security policies and procedures to include new requirements under the Omnibus Rule.
- ☐ Develop or update breach notification policies and procedures in light of the new definition of breach and new requirements and procedures for performing a risk assessment.
- ☐ Provide HIPAA and breach notification training.

If you are not sure whether you are a Covered Entity, BA or Sub BA:

- ☐ Consult legal counsel to determine if you fit any of these definitions under HIPAA.
- ☐ Determine if an established exception, such as the conduit exception, might apply to you.
- ☐ If you are a Patient Safety Organization, Health Information Organization, e-prescribing gateway, or a personal health record vendor, or if you provide data transmission services or facilitate access to a covered entity's records, you should confirm HIPAA's applicability to you and institute the steps needed for HIPAA compliance.
- ☐ Once your status is confirmed, refer to the above checklist applicable to you to get started.