ALSTON&BIRD LLP

WWW.ALSTON.COM

Employee Benefits & Executive Compensation ADVISORY ■

AUGUST 28, 2014

Looming HIPAA Deadline for Business Associate Agreements and Security Risk Assessment

As we catch our breath from the latest Affordable Care Act changes, health plan sponsors should refocus on a couple of important HIPAA requirements that may have previously moved to the back burner—HIPAA security risk assessments and business associate agreement updates. These requirements may create significant risk for employer plan sponsors that fail to comply.

September 23 Deadline for Business Associate Agreement Updates

The HIPAA Omnibus Final Rule (the "Omnibus Rule")[1] became effective March 26, 2013, with a general compliance deadline of September 23, 2013. Compliance with the Omnibus Rule required changes to several HIPAA documents and related compliance practices, including business associate agreements, the HIPAA notice of privacy practices and breach assessment policies and procedures. For more information about other aspects of the Omnibus Rule that apply to employer-sponsored group health plans, see our advisory from March 11, 2013.[2]

With respect to business associate agreements, however, the Omnibus Rule included transition relief that allowed certain health plans an extended transition period within which to make necessary changes to their business associate agreements if certain conditions were met.

To qualify for the transition relief, you must meet two requirements:

- You must have entered into the business associate agreement prior to January 25, 2013 (*the date the Omnibus Rule was issued*); and
- The contract must not have been modified or renewed between January 25, 2013, and September 22, 2014.

---

1 *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules,* 45 Fed. Reg. 5566 (January 25, 2013)

2 Alston & Bird Employee Benefits & Executive Compensation Group, "New HIPAA Omnibus Rule: Issues for Employer Plan Sponsors and Group Health Plans," March 11, 2013, at http://www.alston.com/advisories/HIPPA-Omnibus-Rule.

That transition relief will now expire September 23, 2014 (if it has not already). As of September 23, 2014, all business associate agreements must be updated as necessary to reflect the Omnibus Rule requirements.

Accordingly, covered entities should review their business associate agreements to ensure they have all been updated.

Practice Pointer: Business associate agreement provisions that may require review and updating for compliance with the Omnibus Rule include:

- An update to the definition of PHI;
- Updated subcontractor provisions;
- Provision requiring business associate to comply with the HIPAA Security Rule;
- Breach identification and/or reporting obligations;
- The forms in which documents must be provided following a request to access PHI; and
- Limitations on the use of PHI for marketing.

HIPAA Security Risk Assessments

In light of the recent increase in HIPAA audit/investigation activity and recent large-scale data breaches, employer plan sponsors should redouble their efforts for self-funded health plan HIPAA security compliance. The HIPAA Security Rule requires that each covered entity (i.e., the Plan) and its business associates (i.e., TPAs and other service providers) conduct a thorough and accurate risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (ePHI) held by the covered entity or business associate.[3]

Completion of the risk assessment will likely require input from a number of business functions within the employer plan sponsor or TPA, including Benefits, HR, IT security, HR information systems, Payroll and Legal. The Privacy Officer and the Security Officer (if someone other than the Privacy Officer) are responsible for ensuring that the risk assessment is performed and documented. However, elements of the assessment will likely need to be completed by other groups outside the Plan/TPA's normal workforce (legal, HRIS, IT, privacy office, payroll, etc.).

Practice Pointer: The Security Officer will need to coordinate with many different business groups within the covered entity or business associate. Obtaining buy-in from all these groups will be critical to the successful completion of the HIPAA risk assessment.

[3] 45 C.F.R. § 164.308(a)(1)(ii)(A)

General Security Risk Assessment Requirements

There are numerous methods for performing a risk assessment, and there is no single method or best practice that guarantees compliance. However, there are several elements that a risk assessment must incorporate, regardless of the method employed.

1. ***Scope of the Assessment***

   The covered entity or business associate must perform a thorough risk assessment to determine the potential risks and vulnerabilities to ePHI[4] created, received, maintained or transmitted by the covered entity or business associate.[5]

   For this purpose, risk can be defined[6] as the net mission impact considering (1) the probability that a particular threat will exercise a particular vulnerability and (2) the resulting impact if this should occur. Risk may arise from legal liability or negative impact on the business.

2. ***Data Collection***

   The covered entity or business associate must identify where the ePHI is stored, received, maintained or transmitted.

   The covered entity or business associate can accomplish this by reviewing past and present projects, performing interviews with personnel utilizing PHI, reviewing documentation or using other data gathering techniques.

3. ***Identify and Document Potential Threats and Vulnerabilities***

   The covered entity or business associate must identify and document reasonably anticipated threats to ePHI and system vulnerabilities.[7] For this purpose, threats and vulnerabilities can be defined as:

   - **Threat** – the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability, including natural disasters (e.g., floods, earthquakes and tornadoes), human threats (e.g., malicious software, hackers) and environmental threats (e.g., power failures, pollution and liquid leakage).
   - **Vulnerability** – a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

4. ***Assess Current Security Measures***

   The covered entity or business associate should assess and document the security measures it uses to safeguard ePHI.[8]

   The security measures implemented to reduce risk will vary among organizations based on factors such as the size and complexity of the organization. As a result, the appropriate security measures needed to reduce the likelihood of risk to the security of ePHI will vary from covered entity to covered entity or business associate to business associate.

---

4 This includes ePHI held in forms such as hard drives, CDs, DVDs, smart cards or other storage devices or portable electronic media.

5 45 C.F.R. § 164.306(a).

6 Based on recommendations of the National Institute of Standards and Technology (NIST). Use of definition is not mandatory.

7 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).

8 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).

5. Determine the Likelihood of Threat Occurrence

The Security Rule requires covered entities and business associates to take into account the probability of potential risks to ePHI.[9] The results of the risk assessment, combined with the initial list of threats, will influence the determination of which threats the Security Rule requires protection against because they are reasonably anticipated.

The output in the report for this element should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of ePHI.

6. Determine the Potential Impact of Threat Occurrence

The Security Rule requires consideration of the impact of potential risks to the security of ePHI.[10] Accordingly, the covered entity or business associate must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. The covered entity or business associate can use a qualitative or quantitative method or a combination of the two to measure the impact on the covered entity or business associate.

The covered entity or business associate should document all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect ePHI held by the organization.

7. Determine the Level of Risk

The covered entity or business associate must assign risk levels for all threat and vulnerability combinations identified during the risk analysis. The level of risk should factor both the likelihood that the threat occurs and the resulting impact if the threat occurs.

The output on the report for this part should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level.

8. Finalize Documentation

The covered entity or business associate must document the risk assessment, but HIPAA does not require a specific format.[11]

9. Periodic Review and Update to the Risk Assessment

The covered entity or business associate must continue to monitor its risk assessment in light of new developments.[12] HIPAA does not specify the frequency with which such updates must occur, but they should be driven by circumstances and changes to the environment that could impact ePHI.

---

9 45 C.F.R. § 164.306(b)(2)(iv).

10 45 C.F.R. § 164.306(b)(2)(iv).

11 45 C.F.R. § 164.316(b)(1).

12 45 C.F.R. § 164.316(b)(2)(iii).

HHS Online Security Risk Assessment Tool

One available method for conducting the security risk assessment is to use the Security Risk Assessment Tool ("SRA Tool") offered by the Department of Health and Human Services (HHS). The SRA Tool can be found at http://www.healthit.gov/providers-professionals/security-risk-assessment-tool. The SRA Tool is a software application that is one resource (among other tools and processes) the covered entity or business associate may use to conduct the security risk assessment (or review an existing security risk assessment). Although the SRA Tool was designed for small and medium sized medical practices, the questions are generally applicable to any type of covered entity or business associate.

The SRA Tool is composed of 154 questions covering 12 different compliance categories, including:

- Maintaining your security program;
- Identifying your assets;
- Managing access to your assets;
- Managing the integrity of your ePHI;
- Managing your media;
- Managing your facilities;
- Managing your workforce;
- Educating your workforce;
- Managing your vendors;
- Continuing operations when emergencies occur;
- Auditing your operations; and
- Managing incidents.

The SRA Tool produces a report after questions are completed and can be used to form part of the documentation for your risk assessment. While HHS has made clear that completion of the SRA Tool does not guarantee compliance with the HIPAA security risk assessment requirement, use of this tool should generally assist the organization in conducting, reviewing and documenting risk assessment compliance efforts.

If you would like to receive future *Employee Benefits & Executive Compensation Advisories* electronically, please forward your contact information to **employeebenefits.advisory@alston.com.** Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Members of Alston & Bird's Employee Benefits & Executive Compensation Group

Robert A. Bauman
202.239.3366
bob.bauman@alston.com

Saul Ben-Meyer
212.210.9545
saul.ben-meyer@alston.com

Stacy C. Clark
404.881.7897
stacy.clark@alston.com

Emily Seymour Costin
202.239.3695
emily.costin@alston.com

Patrick C. DiCarlo
404.881.4512
pat.dicarlo@alston.com

Ashley Gillihan
404.881.7390
ashley.gillihan@alston.com

David R. Godofsky
202.239.3392
david.godofsky@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

H. Douglas Hinson
202.239.3432
doug.hinson@alston.com

Emily C. Hootkins
404.881.4601
emily.hootkins@alston.com

James S. Hutchinson
212.210.9552
jamie.hutchinson@alston.com

Johann Lee
202.239.3574
johann.lee@alston.com

Blake Calvin MacKay
404.881.4982
blake.mackay@alston.com

Emily W. Mao
202.239.3374
emily.mao@alston.com

Steven C. Mindy
202.239.3816
steven.mindy@alston.com

Craig R. Pett
404.881.7469
craig.pett@alston.com

Earl Pomeroy
202.239.3835
earl.pomeroy@alston.com

Jonathan G. Rose
202.239.3693
jonathan.rose@alston.com

Syed Fahad Saghir
202.239.3220
fahad.saghir@alston.com

Thomas G. Schendt
202.239.3330
thomas.schendt@alston.com

John B. Shannon
404.881.7466
john.shannon@alston.com

Richard S. Siegel
202.239.3696
richard.siegel@alston.com

Carolyn E. Smith
202.239.3566
carolyn.smith@alston.com

Michael L. Stevens
404.881.7970
mike.stevens@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Elizabeth Vaughan
404.881.4965
beth.vaughan@alston.com

Kerry T. Wenzel
404.881.4983
kerry.wenzel@alston.com

Kyle R. Woods
404.881.7525
kyle.woods@alston.com

ALSTON&BIRD LLP

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 12th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.756.3300 ■ Fax: 202.756.3333