ALSTON & BIRD LLP

WWW.ALSTON.COM

Health Care ADVISORY ■

**OCTOBER 1, 2014**

# HIPAA Audit Program Phase 2 Update

In September, several representatives of the U.S. Department of Health and Human Services Office for Civil Rights (OCR) made presentations that provide important guidance for covered entities and their business associates on the next phase of OCR's HIPAA Audit Program, which has been delayed. The key takeaways:

- Take advantage of the delay in Phase 2 of the Audit Program to address and enhance compliance with the requirements of the Privacy, Security and Breach Notification Rules.
- Make sure to have conducted and/or updated a comprehensive Security Rule risk assessment.
- Take the Audit Program seriously–HIPAA audits may be used as an enforcement tool.

## Previously Announced Plans for Phase 2

Earlier this year, OCR had announced that Phase 2 of the Audit Program would begin this year and would target specific high risk issues. It indicated that, beginning this past summer, it would conduct a pre-audit survey of 800 covered entities and 400 business associates to determine suitability for the Audit Program.[1] OCR stated it would use the survey to select 350 covered entities and 50 business associates to be audited in Phase 2, with audits distributed across health plans, health care providers and clearinghouses (for covered entities) and across IT-related and non-IT related business associates. At the same time, OCR's plans were to begin Phase 2 audits of covered entities in the fall of 2014, with 2014 audits of covered entities focused on the following:

- Risk analysis and risk management (Security Rule)
- Notice of privacy practices and access rights (Privacy Rule)
- Content and timeliness of breach notification (Breach Notification Rule)

The 2015 audits of covered entities would focus on device and media controls and transmission security (Security Rule) as well as safeguards and training on policies and procedures (Privacy Rule). Audits of business associates were scheduled to start in 2015, focused on risk analysis and risk management (Security Rule) and breach reporting to the covered entity (Breach Notification Rule).

---

[1] See our blog post on OCR's pre-audit survey at: http://www.alstonprivacy.com/blog.aspx?entry=5231.

At the time, OCR had also indicated that most audits would be "desk audits" (i.e., document-only audits, without follow-up) in which the entity would be required to respond to data request letters within two weeks of receiving the request. The audits would be conducted with audit protocols updated to reflect the HIPAA/HITECH Act Omnibus Rule changes, as well as to provide more specific test procedures. The protocols would also use a sampling methodology to assess compliance with a number of provisions. OCR promised that the updated audit protocols would be made available on its website so that covered entities and business associates could use the protocols to assess their compliance efforts.

## A New Web Portal and Expanded Plans for Phase 2

OCR has recently announced that Phase 2 of the Audit Program has been delayed and that, when it starts, there will be more on-site, comprehensive audits and fewer desk audits than previously planned.

Early in September, the OCR senior health information privacy advisor who heads the Audit Program announced that OCR has delayed the pre-audit survey, as well as Phase 2 of the Audit Program, until OCR is able to implement a new web portal through which entities can submit information. OCR is planning to use its new portal to conduct the pre-audit survey screening tool as well as have entities enter data for the audits. According to OCR, the portal technology will help it streamline the audit process by collecting, collating and analyzing audit data. The portal is intended to save OCR time and allow it to conduct more audits.

While OCR had previously planned to begin Phase 2 of its Audit Program (the permanent audit program) in 2014, OCR now is not specifying when the surveys will be issued or when Phase 2 will begin, although some pre-audit surveys could be distributed in the near future. Accordingly, covered entities and business associates are advised to stay tuned.

In addition to delaying the start of Phase 2 of the Audit Program, OCR has changed its plans for the audits. While it appears that most audits will still be desk audits, OCR, with the new web portal and possibly some additional funding, is planning to conduct more on-site, comprehensive audits (including audits of business associates) than previously planned and may conduct many fewer desk audits.

OCR still plans to conduct a pre-screening survey of covered entities and business associates that are potential candidates for audits in Phase 2 of the Audit Program. This survey is likely to occur "in the near future," and responses will be collected by means of OCR's new portal.

OCR advises covered entities to be ready with a list of their business associates, contact information for the business associates and the services provided by the business associates. It appears that the list of business associates to be surveyed and/or audited will be derived from the lists of business associates provided by surveyed and/or audited covered entities.

While the Audit Program pilot was conducted by contractors, Phase 2 will be staffed and conducted by OCR personnel. Covered entities will be responsible for demonstrating compliance with the Security Rule (including a risk analysis), the Privacy Rule (including access issues) and breach notification under the Breach Notification Rule. Among other things, OCR will be looking for comprehensive, periodic risk analyses and documentation of appropriate follow-up risk management plans and activities. Business associate audits may focus on compliance with requirements such as security risk assessments and breach notifications.

In conducting its audit work, OCR will look not only for written policies and procedures, but also for evidence of compliance, such as evidence that the policies and procedures have been implemented and are being enforced, e.g., by the imposition of sanctions (consistent with the entities' sanctions policies) for violations. It is also likely to be important for covered entities and business associates to be able to demonstrate that they have periodically reviewed and updated their policies and procedures in light of their experience, changes in their operations and information technology environment and/or changes in applicable law. Because OCR plans to move the audits quickly and many

of the audits will remain desk audits, covered entities and business associates may not be able to supplement or clarify their initial responses to audit inquiries, unlike in the Audit Program pilot. Accordingly, the content of the initial response is crucial. Covered entities and business associates should contact legal counsel for assistance in preparing written submissions to OCR, especially their initial responses to OCR.

OCR will update its HIPAA audit protocols before this next round of audits begin.

## HIPAA Audits: Part of OCR's Arsenal of Enforcement Tools

Earlier this month, an OCR representative had indicated, in response to questions concerning how OCR decides whom to audit, that OCR does not see audits as a direct enforcement arm and that audits would not be performed on organizations that are the subject of an open breach or HIPAA compliance investigation. This does not mean that such audits hold no enforcement implications. More recently, another OCR representative made it clear that "[the Audit Program] will be an enforcement tool," indicating that HIPAA audits will become a means to begin compliance investigations of covered entities and business associates.

During the Audit Program pilot, OCR had indicated that it viewed HIPAA audits mainly as a compliance improvement activity, designed to help OCR determine the types of technical assistance that need to be developed and the types of corrective action that are most effective. OCR had also indicated that it would seek to audit a wide range of covered entities in terms of size, geographic distribution and type (individual and institutional health care providers, a wide variety of health plans and health care clearinghouses).[2]

As the Audit Program progresses and continues to evolve, covered entities and business associates should expect that OCR will use audits as an enforcement tool and may pursue compliance reviews and/or investigations of entities for serious compliance issues or violations identified during an audit. Keep in mind that compliance reviews and investigations can lead to the imposition of civil money penalties or resolution agreements involving the payment of resolution amounts. Consequently, covered entities and business associates should currently expect–at a minimum–that:

- A failure to respond appropriately to an audit request may lead to a compliance review or enforcement action; and
- If an audit reveals a significant or serious compliance issue, OCR may undertake a more comprehensive compliance review.

## Coming HIPAA Guidance

- OCR is working on guidance for covered entities and business associates on a number of HIPAA topics, including:
- Breach notification safe harbors
- Breach risk assessment tool
- HIPAA minimum necessary requirements
- HIPAA marketing rules

---

[2] For background on OCR's Audit Program pilot, see our November 30, 2011, blog post at: http://www.alstonprivacy.com/blog.aspx?entry=4498.

## Be Prepared

Given the number of audits OCR plans to conduct in Phase 2 of the Audit Program, the likelihood that any particular covered entity or business associate will be audited in Phase 2 is relatively low. However, as noted above, OCR views audits as a tool in its compliance and enforcement arsenal. Covered entities and business associates should consequently be prepared for HIPAA audits and consider taking advantage of the delay in Phase 2 to review their HIPAA compliance programs and:

- Ensure that privacy and security policies and procedures reflect current HIPAA requirements (including the HIPAA/HITECH Act Omnibus Rule[3]) and update such policies and procedures, as needed, taking into consideration any changed circumstances.
- Conduct or update comprehensive Security Rule risk assessments and ensure that risk mitigation and management plans are up to date, including with respect to new technology implemented since the prior risk assessment. If needed, create a corrective action plan to address HIPAA compliance issues.
- Review compliance in other high risk areas, especially those on which OCR is likely to focus audit attention, including:
  - Privacy Rule: Notice of privacy practices, individual access rights, implementation of the minimum necessary requirements and authorizations.
  - Security Rule: Media and device movement and disposal, transmission security, audit controls and monitoring.
  - Breach Notification Rule: Content and timeliness of breach notification.
- Consider encryption of electronic transmissions, mobile devices and media containing electronic protected health information, particularly USB/thumb drives. This is a safeguard specifically mentioned by OCR representatives.
- Review covered entity/business associate relationships for HIPAA compliance.
- Review training materials and ensure workforce training is up to date and documented.
- Ensure proper documentation of compliance with policies and procedures, including training, complaint handling and resolution, application of sanctions policy, etc.

While the HIPAA audit delay announcements may cause a sigh of relief among some covered entities and business associates, now is the time to prepare. OCR will conduct more on-site audits and fewer desk audits than previously planned, the audits are part of OCR's enforcement arsenal and the outcomes could lead to sanctions and monetary fines. Alston & Bird stands ready to assist with reviewing and updating HIPAA policies and procedures; enhancing HIPAA compliance; responding to OCR during a HIPAA audit, compliance review or investigation; and interacting with OCR regarding audit, corrective action and/or enforcement efforts. Please let us know how we can help you get ready.

*Written by **Paula M. Stannard**, **Angela T. Burnette** and **Julia Dempewolf**.*

---

[3] For a discussion of the HIPAA/HITECH Act Omnibus Rule, please see our January 25, 2013, Health Care Advisory, Overview of the HIPAA/HITECH Omnibus Final Rule, and our February 1, 2013, HIPAA/HITECH Act Omnibus Rule Checklist, both of which are available on our website.

If you would like to receive future ***Health Care Advisories*** electronically, please forward your contact information to **healthcare.advisory@alston.com.** Be sure to put "**subscribe**" in the subject line.

If you have any questions, or would like additional information, please contact any of the following:


David S. Abernethy
202.239.3987
david.abernethy@alston.com

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

Joshua L. Becker
404.881.4732
josh.becker@alston.com

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

Donna P. Bergeson
404.881.7278
donna.bergeson@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Michael L. Brown
404.881.7589
mike.brown@alston.com

Cathy L. Burgess
202.239.3648
cathy.burgess@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Jennifer L. Butler
202.239.3326
jennifer.butler@alston.com

Mark Timothy Calloway
704.444.1089
mark.calloway@alston.com

Craig Carpenito
212.210.9582
craig.carpenito@alston.com

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

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

Robert J. Dole
202.654.4848
bob.dole@alston.com

Theodore B. Eichelberger
404.881.4385
ted.eichelberger@alston.com

Dan Elling
202.239.3530
dan.elling@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Larry Gage
202.239.3614
larry.gage@alston.com

Ashley Gillihan
404.881.7390
ashley.gillihan@alston.com

David R. Godofsky, F.S.A.
202.239.3392
david.godofsky@alston.com

James A. Harvey
404.881.7328
jim.harvey@alston.com

Katherine E. Hertel
213.576.2600
kate.hertel@alston.com

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

H. Douglas Hinson
404.881.7590
doug.hinson@alston.com

Sean C. Hyatt
404.881.4410
sean.hyatt@alston.com

Bill Jordan
404.881.7850
bill.jordan@alston.com

Ted Kang
202.239.3728
edward.kang@alston.com

Peter M. Kazon
202.239.3334
peter.kazon@alston.com

David Keating
404.881.7355
david.keating@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

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Wade Miller
404.881.4971
wade.miller@alston.com

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

William (Mitch) R. Mitchelson, Jr.
404.881.7661
mitch.mitchelson@alston.com

Michael H. Park
202.239.3630
michael.park@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

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

Earl Pomeroy
202.239.3835
earl.pomeroy@alston.com

Steven L. Pottle
404.881.7554
steve.pottle@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

J. Mark Ray
404.881.7739
mark.ray@alston.com

Mark H. Rayder
202.239.3562
mark.rayder@alston.com

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

Colin Roskey
202.239.3436
colin.roskey@alston.com

Sam Rutherford
404.881.4454
sam.rutherford@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Marc J. Scheineson
202.239.3465
marc.scheineson@alston.com

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

Thomas A. Scully
202.239.3459
thomas.scully@alston.com

Donald E. Segal
202.239.3449
donald.segal@alston.com

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

Dominique Shelton
213.576.1170
dominique.shelton@alston.com

Robert G. Siggins
202.239.3836
bob.siggins@alston.com

Carolyn Smith
202.239.3566
carolyn.smith@alston.com

Perry D. Smith, Jr.
404.881.4401
perry.smith@alston.com

Paula M. Stannard
202.239.3626
paula.stannard@alston.com

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

Brian Stimson
404.881.4972
brian.stimson@alston.com

Robert D. Stone
404.881.7270
rob.stone@alston.com

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

Julie K. Tibbets
202.239.3444
julie.tibbets@alston.com

Timothy P. Trysla
202.239.3420
tim.trysla@alston.com

Kenneth G. Weigel
202.239.3431
ken.weigel@alston.com

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

Michelle A. Williams
404.881.7594
michelle.williams@alston.com

Marilyn K. Yager
202.239.3341
marilyn.yager@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 ■ 15th 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, CA 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