Employee Benefits & Executive Compensation ADVISORY

March 7, 2012

HIPAA Covered Health Plans Beware: HHS Office of Civil Rights Kicks Off HIPAA Audit Program

Since November 2011, the U.S. Department of Health and Human Services (HHS), through its Office for Civil Rights (OCR), has been conducting audits of covered entities (the "HIPAA Audit Program") for compliance with the privacy and security requirements under HIPAA[1] and the HITECH Act[2] (collectively, the "Privacy & Security Rules").[3] While the Internal Revenue Service and the Department of Labor have conducted audits with respect to HIPAA's portability requirements in the past, the HIPAA Audit Program is a new enforcement effort for HHS/OCR,[4] which until now relied mainly on complaint-based investigations and reviews. This advisory summarizes the HIPAA Audit Program as we currently understand it and provides some basic compliance reminders that may be helpful in preparing for such an audit.

General Overview

As a pilot program, the initial phase of the HIPAA Audit Program consists of 20 audits that are intended to fine-tune OCR's audit protocols. Upon completion of the initial phase (which we understand has been completed or is near completion), OCR intends to use its revised audit protocols to conduct up to 130 additional audits in 2012. OCR has engaged KPMG, a national accounting firm, to develop audit protocols and assist in operating the HIPAA Audit Program.

For 2012, the HIPAA Audit Program is targeting a wide range of types and sizes of covered entities in order to make a broad assessment of Privacy & Security Rule compliance. OCR expects to expand its scope of audits to include business associates in the future.

---

1 Health Insurance Portability and Accountability Act of 1996.

2 Health Information Technology for Economic and Clinical Health (HITECH) Act.

3 See http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.

4 The U.S. Department of Labor, Internal Revenue Service and HHS have joint enforcement authority as to HIPAA's portability requirements (e.g., special enrollment rights and nondiscrimination in eligibility, etc.). As to the Privacy & Security Rules, however, HHS has sole enforcement authority.

Audit Parameters and Consequences

When a covered entity such as a health plan is selected for an audit, OCR will notify the covered entity in writing. The audit notification will explain the audit process and expectations, and request the production of certain documents and information. OCR expects covered entities that are selected for the audit to produce the requested documents and information within 10 business days.

Audited entities can expect an onsite review that may take between three and 10 business days, depending on the complexity of audited entity and the auditor's need to access materials, observe operations and meet with individuals, including:

- interviews with the entity's leadership, such as the chief information officer, privacy officer, legal counsel and health information management/medical records director;
- examinations of the entity's physical features, operations and adherence to its policies; and
- observation of the entity's compliance with HIPAA regulatory requirements.

After completion of the onsite visit, the auditor will provide the covered entity with a draft final report that describes its findings, which may include a list of alleged violations of the Privacy & Security Rules. A covered entity will generally have 10 business days in which to review and provide any written comments to the auditor. The auditor will then complete its final audit report, generally within 30 business days after the covered entity's response and submit it to OCR. In the event the audit report indicates a serious compliance issue, OCR may initiate a formal compliance review to address that issue.

OCR has indicated that the primary purpose of the HIPAA Audit Program is to promote compliance improvements and that it will not post a list of audited entities or audit results that clearly identify the audited party. OCR, however, retains the authority to impose severe sanctions on violators, including (i) injunctions, (ii) imposition of $100-per-violation penalties (up to $50,000 per incidence for willful neglect) that can accrue until correction (with a $1.5 million calendar-year cap for all violations of the same regulatory requirement) and (iii) criminal penalties for knowing violations.

Internal Compliance Review

With the HIPAA Audit Program underway, covered entities and business associates should take this opportunity to "brush the dust off" their HIPAA policy and procedures manuals and other implementation documentation. We suggest preparing by identifying all of the HIPAA policies, procedures and documentation and reviewing them for compliance with the Privacy & Security Rules. Such actions should, at a minimum, include the identification and review of the following (this is a non-exhaustive list):

- HIPAA notice of privacy practices;
- identification of HIPAA privacy and security official(s) and documentation of their authority (e.g., appropriate resolutions appointing and authorizing such individuals);

- plan document(s), including any amendment(s) relating to HIPAA privacy and security (for group health plans);
- HIPAA business associate agreements;
- identification of employees authorized to access protected health information (PHI) and documentation of their HIPAA training, attendance and training materials;
- updated policies implemented to address potential HIPAA breaches;
- written policies and procedures that are designed to comply with the Privacy & Security Rules and that documents, in detail, all of the entity's HIPAA privacy and security practices, including those relating to:
  - the use, disclosure, maintenance, documentation and safeguard measures (administrative, physical and technical) with regard to all PHI;
  - prevention, detection, containment and correction of security violations (including breach under the HITECH Act);
  - contingency and backup plans, and emergency access to electronic information systems;
  - employee training; and
  - sanctions for employees who violate the covered entity's HIPAA policies or procedures;
- documentation of required HIPAA privacy and security risk assessments and analyses on which the HIPAA compliance policies and procedures are based; and
- documentation of actions taken in accordance with the HIPAA policies and procedures, including documentation of identification, investigation and resolution of HIPAA security incidents and complaints.

For further information on HIPAA and HITECH compliance obligations, see our prior advisories linked below:

Employee Benefits & Executive Compensation Advisory: Life's a Breach: What Constitutes a Breach under the HIPAA HiTech Breach Notification Requirements

Employee Benefits & Executive Compensation Advisory: Stimulus Act Imposes Increased HIPAA Obligation on Health Benefit Plans and Service Providers

This advisory was written by* Johann Lee *and* John Hickman*.

ALSTON+BIRD LLP

If you would like to receive future *Employee Benefits and Executive Compensation Advisories* electronically, please forward your contact information including e-mail address 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 one of the following:

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

John R. Anderson
202.239.3816
john.anderson@alston.com

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

Saul Ben-Meyer
212.210.9545
saul.ben-meyer@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
404.881.7590
doug.hinson@alston.com

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

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

David C. Kaleda
202.239.3329
david.kaleda@alston.com

Johann Lee
202.239.3574
johann.lee@alston.com

Brandon Long
202.239.3721
brandon.long@alston.com

Douglas J. McClintock
212.210.9474
douglas.mcclintock@alston.com

Blake Calvin MacKay
404.881.4982
blake.mackay@alston.com

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

Earl Pomeroy
202.239.3835
earl.pomeroy@alston.com

Craig R. Pett
404.881.7469
craig.pett@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

Jahnisa P. Tate
404.881.7582
jahnisa.tate@alston.com

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

Laura G. Thatcher
404.881.7546
laura.thatcher@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

Members of Alston & Bird's Health Care Group

ATLANTA

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

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

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

Kim McWhorter
404.881.4254
kim.mcwhorter@alston.com

D'Andrea J. Morning
404.881.7538
dandrea.morning@alston.com

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

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

Esther Yu
404.881.4240
esther.yu@alston.com

WASHINGTON D.C.

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

ATLANTA
One Atlantic Center
1201 West Peachtree Street
Atlanta, GA 30309-3424
404.881.7000

BRUSSELS
Level 20 Bastion Tower
Place du Champ de Mars
B-1050 Brussels, BE
Phone: +32 2 550 3700

CHARLOTTE
Bank of America Plaza
Suite 4000
101 South Tryon Street
Charlotte, NC 28280-4000
704.444.1000

DALLAS
2828 N. Harwood St.
Suite 1800
Dallas, TX 75201
214.922.3400

LOS ANGELES
333 South Hope Street
16th Floor
Los Angeles, CA 90071-3004
213.576.1000

NEW YORK
90 Park Avenue
New York, NY 10016-1387
212.210.9400

RESEARCH TRIANGLE
4721 Emperor Boulevard
Suite 400
Durham, NC 27703-8580
919.862.2200

SILICON VALLEY
275 Middlefield Road
Suite 150
Menlo Park, CA 94025-4004
650.838.2000

VENTURA COUNTY
Suite 215
2801 Townsgate Road
Westlake Village, CA 91361
805.497.9474

WASHINGTON, D.C.
The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202.239.3300

www.alston.com