# Healthcare regulatory compliance

## Two Approaches for Evaluating HIPAA Compliance

**"The Omnibus Rule will have a direct impact on the compliance efforts of all covered entities and business associates."**

**– Matthew Sadler, Director, KPMG LLP**

**What is the omnibus rule?**
The Final HIPAA Omnibus Rule is essentially an extension of the HIPAA regulations that adds increased protections for Private Health Information (PHI) and imposes significant changes on the HITECH Act.

The Rule also imposes a heightened breach standard, extends liability to business associates and their subcontractors, and requires covered entities to modify existing and future business associate agreements.

**? Did you know?**
KPMG was the ONLY firm selected to work with OCR to develop and implement the compliance Audit Protocol in 2012.

### Would your organization pass a regulatory audit today?

If managing the compliance risks of HIPAA and HITECH wasn't difficult enough, covered entities and their business associates now must also ensure that they stand up to the heightened requirements of the Final HIPAA Omnibus Rule. Yet our experience suggests that many organizations may not fully understand the implications that the Omnibus Rule will have on their compliance efforts.

At KPMG LLP (KPMG), we provide a range of services to help covered entities and their business associates come to terms with their current state of compliance with the HIPAA/HITECH/Omnibus regulations.

For those organizations looking to begin the process or simply evaluate existing processes, capabilities, and controls to drive real and sustainable improvements and enhancements to their privacy and security programs, we provide a proprietary **Mock Audit Program**[1] that is based on the same Office for Civil Rights (OCR) Audit Protocol used by KPMG to conduct the discovery audits of 115 covered entities in 2012.

### Approach #1: Mock Audit Program

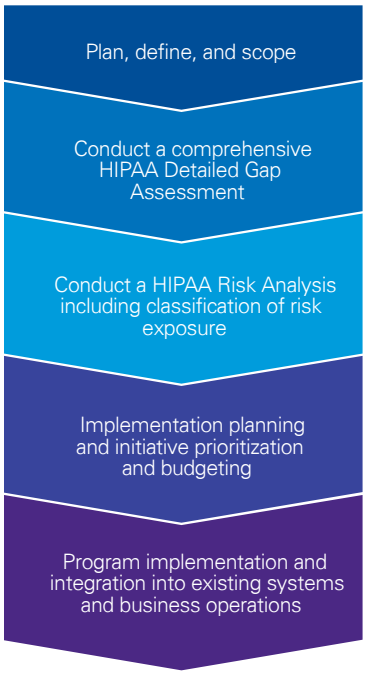

**Are you confident in your readiness for an OCR audit?**

- **Have you performed an assessment** of your organization's current compliance posture in relation to HIPAA, HITECH, and the Omnibus Rule?
- **Have you implemented a certified Meaningful Use system** and, if so, have you updated your risk assessment to meet the Meaningful Use Criteria?
- **Are your organization's risk management programs and protocols** proactive and collaborative?
- **Are you confident that your Information Security and Privacy policies** and procedures as well as your notice of privacy practices and business associate agreements are robust and appropriate?
- **Has your organization had any recent privacy- and/or security-related issues** that may have resulted in a breach or other noncompliance-related event?

[1] *A mock audit does not constitute an examination under AICPA attestation standards. Accordingly, we will not express an opinion or conclusion or provide any form of assurance on any regulatory matters.*

**"Checking your readiness to react to an audit request from OCR now can help you not only comply with requests of this nature that may occur in the future, it can also help identify missing or incomplete program attributes that your organization leverages in order to comply with the Rule."**

**– Jaime Pego, Director, KPMG LLP**




### Did you know?

? OCR expects that the scope of the HIPAA Risk Assessment must include PRIVACY in addition to security.

### Approach #2: HIPAA Risk Assessment

For those organizations seeking to perform an assessment as necessary in the regulatory requirements of the HIPAA Omnibus Rule, we also offer a **HIPAA Risk Assessment** service that leverages our first-hand experience and deep regulatory insight to help organizations create and maintain sustainable HIPAA compliance programs.

#### HIPAA Risk Assessment

At KPMG, we understand what is required to conduct a robust risk assessment and have keen insight into why certain risk assessments fail to satisfy the standards set by OCR. That is why our approach:

- Incorporates both security and privacy within the scope of the assessment;
- Focuses heavily on interviews to properly understand the full context of risks and controls within the operating structure;
- Validates the nature of the control operations through thorough walk-throughs; and
- Documents the practices and identified gaps to meet document retention requirements.

### Why KPMG? Our client chose us because:

**We provide objective compliance assessments:** As a recognized and trusted third-party adviser, we take an objective view of your compliance program to identify gaps and develop strategies for mitigating them.

**We base our methodolgies on real experience:** Our team is highly experienced in HIPAA, HITECH, and Omnibus Rule strategies, processes, and tools, and continuously leverage their deep experience to deliver measurable value to our clients.

**We have tools that can deliver valuable insights:** Our tools and methodology are based on our experience in defining the performance criteria for compliance to HIPAA as well as developing the OCR Audit Protocol used during the 2012 performance audits.

**We take a flexible approach:** We tailor the features and scope of our observations and recommendations to fit each client's unique needs.

## For more information, contact:


**Michael Ebert**
**Partner, Healthcare Advisory**
**T:** +267-256-1686
**E:** mdebert@kpmg.com

**Jaime Pego**
**Director, Healthcare Advisory**
**T:** +973-912-4507
**E:** jpego@kpmg.com

**Matthew Sadler**
**Director, Healthcare Advisory**
**T:** +717-260-4617
**E:** msadler@kpmg.com

**Chris Jurs**
**Manager, Healthcare Advisory**
**T:** +631-425-6506
**E:** cjurs@kpmg.com

**Mark Johnson**
**Managing Director, Healthcare Advisory**
**T:** +615-248-5548
**E:** mmjohnson@kpmg.com


**kpmg.com/socialmedia**