The Department of Health and Human Services (HHS) Office of Civil Rights (OCR) has been very busy in 2016, making big changes in the world of HIPAA compliance. This year, OCR has already issued landmark fines for HIPAA violations, completed a total reconstruction of its HIPAA audit protocol guidance, and released a business associate listing template. It is critical that healthcare organizations and the businesses that support them are aware of all the changes around the HIPAA Audit Protocol 2.0.

With these organizations in mind, Focal Point has identified the new HIPAA audit protocol as one of the hottest privacy topics to monitor.

HIPAA Audit Protocol 2.0
With the official kick-off of the Phase 2 HIPAA Audit Program in early 2016, OCR released new and improved protocol for all its audits. Although these audits will evaluate covered entities and business associates varying in size and complexity, the updated protocol will prove to be especially useful for smaller providers and practices, which are often less prepared to address the overwhelming number of required policies, documents, and practices.

This document identifies the following considerations around this important update:

- Parties who should consider the updated protocol,
- Notable protocol updates, and
- Recommended next steps.

This document is for informational purposes only and should not be taken as specific legal advice.
HIPAA in the News: HIPAA Audit Protocol 2.0

Who Should Consider the New Protocol?
While OCR will only use this protocol when performing Phase 2 Audits on the 500 - 800 selected entities, all covered entities and their business associates should take this protocol into consideration. OCR has essentially made the keys to HIPAA compliance accessible to everyone, and it would be to the advantage of all entities to be proactive and implement them.

What Are the Key Changes?

Omnibus Rule Requirements
The new audit protocol reflects the updated Omnibus Rule changes that went into effect in 2013. This includes modifications related to uses and disclosures that require an authorization, and places responsibility on business associates to comply with HIPAA requirements.

More Prescriptive Guidance
OCR has taken this 2016 update as an opportunity to build out the 2012 audit protocol by including more robust guidance across an expanded number of requirements. The new protocol also provides more detailed procedures related to the processes and documentation that should be in place and key issues healthcare organizations should consider. Most of the notable changes are around the documentation, by way of policies, that OCR expects organizations to have in place.

Entity Designation
This new update distinguishes whether requirements are applicable to covered entities, business associates, or both designations. This is one of the most useful updates in the protocol, since there is often confusion among business associates as to whether or not the Privacy Rule requirements apply to them.

Procedures for Rule Requirements
The 2016 audit protocol outlines procedures for gathering and documenting information on relevant areas of focus for the following requirements:

Privacy Rule
- Notice of Privacy Practices
- Individual’s Right to Request Restrictions of Uses and Disclosures
- Individual’s Right to Request Confidential Communications
- Individual’s Right to Request an Amendment to PHI
- Individual’s Right to Request an Accounting of Disclosures
- Administrative Requirements
- Uses and Disclosures of PHI

Security Rule
- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards

Breach Notification Rule
What are the Next Steps?

Regardless of whether your organization has received a pre-screen audit questionnaire from OCR, proactive measures should be taken to leverage the information in the new audit protocol to ensure your organization is working to meet these standards. Here are some steps your organization can take:

1. Perform an internal assessment or engage a third party to evaluate your alignment with the audit protocols. This will help identify protocol requirements your organization needs to address and “quick wins” that can move the organization one step closer to compliance.

2. Leverage the new audit protocol to your organization’s benefit. The protocol places a heavy emphasis on the policies and procedures organizations must have in place. Review your documented policies and procedures and ensure that all elements outlined in the protocol are addressed. If your organization does not have policies and procedures in place, create a timeline for their development and communicate this to your employees.

3. If your organization has not performed a risk analysis to identify potential vulnerabilities or threats to its IT infrastructure, now is the time to perform one. The new audit protocol encourages organizations to have a risk analysis performed, documented, and reviewed.

About Focal Point LLC

Focal Point Data Risk is a new type of risk management firm, one that delivers a unified approach to addressing data risk through a unique combination of service offerings. Focal Point has brought together industry-leading expertise in cyber security, identity governance and access management, data privacy and analytics, internal audit, and hands-on training services, giving companies everything they need to plan and develop effective risk and security programs. By integrating these services, we provide our clients with the flexible support they need to protect and leverage data across any part of their organization. Simply put, Focal Point is the next generation of risk management.

Eric Dieterich, Privacy Practice Leader
786.390.1490 | edieterich@focal-point.com

Data Privacy Services

- Privacy Risk Assessments
- HIPAA Compliance
- Privacy Office Services
- Corrective Action Plan Audits
- Cross Border Transfer Assessments
- Breach Notification Procedures
- Privacy Awareness Training
- Policy Development