

A photograph of a male doctor with grey hair and glasses, wearing a white lab coat over a blue shirt and tie. He is smiling and holding a stethoscope to the chest of a young girl with long brown hair, who is also smiling. The girl is wearing a light blue button-down shirt and jeans. They are in a bright, clinical setting with large windows in the background.

## **Phase II HIPAA Audits: Leave the Sink in the Kitchen**

*By Adam Bullian, JD*





## **Phase II HIPAA Audits: Leave the Sink in the Kitchen**

*By: Adam Bullian, JD*

The Phase II HIPAA Audits are expected to start very soon. This document is a primer on where we have been, where we are going, and what you can do now to prepare for a Phase II Audit.

### **Phase I Audits: Where have we been?**

While the overall goal is to prepare for the HIPAA Phase II Audits, it is important to briefly look at the Phase I Audits. If nothing more than to know how the upcoming round will be different.

The Phase I HIPAA Audits were completed in 2011 and 2012. That round included only 115 organizations. It included health plans, healthcare clearinghouses, and providers. No business associates were included in Phase I. These audits were comprehensive; in that they covered the Security Rule, Privacy Rule, and Breach Notification Rule. They were completed on site by a contractor of the Office of Civil Rights (“OCR”); the organization tasked with HIPAA enforcement. Looking just at the providers that were audited in Phase I, there were a total of 61 organizations.

Of those, 59 had at least one negative finding in the audits. Of all 115 organizations audited, OCR found that only 11% had no negative findings. In other words, widespread issues were found with all organizations audited. Providers had the most difficult time with compliance of all three types of covered entities, and of those, small providers had the most egregious issues.

For providers, the security rule was where most negative findings were identified. According to OCR, the most common cause of negative findings was because the entity was “unaware of the requirement.” However, OCR has continually held to the notion that ignorance of the requirements is not a defense. Therefore, organizations with negative findings were still cited, regardless of the fact that they were unaware of the requirements.

### **Phase II Audits: Where are we going?**

According to the latest information from OCR, Phase II of the HIPAA Audits are set to begin very soon. They will be conducted by a contractor, and will primarily be desk audits. The audits are projected to run through 2016, in several cycles. They will include a total of 350 Covered Entities and 50 Business Associates over the course of this Phase.

### **How to Prepare for Phase II Audits**

**A. Identify Business Associates:** OCR is expected to ask every Covered Entity audited for a list of its Business Associates. This is anticipated to compile the list of Business Associates from which



some will be audited. Therefore, it is best to have this list available as soon as possible. There will not be a great deal of time for production of documents after requested, and this information can be scattered in organizations. The time to prepare this list is now.

**B. Include Dates on all Documentation of Compliance Program:** OCR is looking for a current, ongoing, and comprehensive HIPAA compliance program. Not a one-time project. Therefore, ensure all documentation of your HIPAA Compliance Program is dated as of the last time reviewed. Better yet, they should include multiple dates; thus indicating that they have been periodically reviewed.

**C. Documentation Should Accurately Reflect the Compliance Program:** Auditors will not contact organizations for clarification of documents after they have been submitted. Therefore, what is submitted must accurately and comprehensively demonstrate the completeness of an ongoing compliance program.

**D. Only Submit What Is Requested:** Leave the sink in the kitchen. Give the auditor what they ask for, and little – if nothing – more. Extraneous information could confuse the reviewer, and lead to a more in depth compliance review.

**E. Have a Current Risk Assessment:** This is a fundamental requirement of the Security Rule, and is absolutely necessary for compliance .

**F. Notice of Privacy Practices:** A Notice of Privacy Practices must meet all requirements, be posted in waiting areas and online. Additionally, organization should have policies and procedure that outline documentation of receipt.

**G. Policies and Procedures for Individual Access:** Ensure they are in place and up to date.

**H. Incident Response Policies and Procedures:** Ensure policies and procedure in response to an incident are in place. Have members of an incident response team identified and ensure they understand their roles and responsibilities.

In closing, there is much to do to be prepared for a HIPAA audit, and time is running out. It is best to prepare now. A hurried response to audit request will likely lead to poor performance.



## About the Author:

Adam Bullian brings years of regulatory compliance experience in healthcare and HIPAA. He has assisted organizations in creating compliance programs, developing lobbying strategies, and workforce training programs. His commitment to healthcare issues has been apparent throughout his career; from being involved in the earliest state implementation efforts of the Affordable Care Act, to the founding of a non-affiliated political action committee. He holds a Bachelor's Degree in History and Political Science from West Virginia University, and a Juris Doctorate Degree from the West Virginia University College of Law.

*Adam Bullian, JD*  
*abullian@qipsolutions.com*

## About QIP Solutions:

Based in the Washington D.C. metro area, with partners nationwide, QIP draws from deep professional experience in healthcare information technology and security, risk management, audit, and legal practice. QIP Solutions provides clear, cost-effective, and comprehensive solutions to healthcare compliance solutions through its QI Express SaaS platform. For more information, please visit our website at **qiexpress.com** or e-mail **info@qipsolutions.com**.

## Disclaimer:

The material provided in this document is intended for informational and educational purposes only and does not constitute legal advice or legal opinion. These materials are intended, but not promised or guaranteed to be current, complete, or up-to-date and should in no way be taken as an indication of future results or activities. Transmission of this information is not intended to create, and the receipt does not constitute, an attorney-client relationship between reader and the author or QI Partners, LLC. You should not act or rely on any information contained in this document without first seeking the advice of an attorney or HIPAA compliance professional.