Form Approved
OMB No. 0945-xxxx
Exp. Date XX/XX/20XX

OCR HIPAA Audit Covered Entity Survey

Page 1 – Introduction

The purpose of this survey is to obtain your feedback, as an audited covered entity, on the HIPAA Compliance Audit Program conducted by KPMG under contract with the Office for Civil Rights (OCR), Department of Health and Human Services. Information obtained from you in response to this survey will only be used to assess the audit program and will not be used to further assess your entity's HIPAA compliance or affect your chance of being selected for additional review by OCR.

OCR requests one collective response from your organization. If multiple individuals at your organization oversee different aspects of HIPAA compliance (e.g. privacy officer, security officer, etc.) please consult with those persons while completing this survey.

The survey consists of 17 questions and should take approximately 15-40 minutes to complete. It has been approved by the Office of Management and Budget (OMB). (Control ######)

OCR has contracted PricewaterhouseCoopers, LLP to conduct the survey and aggregate the results. Questions about the survey may be directed to Erika Ball, Erika.L.Ball@us.pwc.com. Questions about the HIPAA audit program may be directed to Linda Sanches, Linda.Sanches@hhs.gov, Office for Civil Rights, Department of Health and Human Services.

Page 2 – Overall Impressions

The following statements relate to your overall impression of the HIPAA audit process.

1. Please indicate the level to which you agree with each of the following statements.

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
The audit process was appropriate for assessing HIPAA compliance for our type of entity.	❍	❍	❍	❍	❍	❍
The auditors were well-prepared for the audit and were knowledgeable about HIPAA Privacy Rule.	❍	❍	❍	❍	❍	❍
The auditors were well-prepared for the audit and were knowledgeable about HIPAA Security Rule.	❍	❍	❍	❍	❍	❍
The auditors were well-prepared for the audit and were knowledgeable about the Breach Notification Rule.	❍	❍	❍	❍	❍	❍
Communications received throughout the audit clearly explained what was required of our personnel.	❍	❍	❍	❍	❍	❍

Page 3 – Pre-Audit and Audit

The following questions relate to your knowledge about the HIPAA audit program and your actions taken to assess or improve HIPAA compliance, prior to and during the audit.

2. Please indicate the time period during which you became aware of the audit program. If you became aware of the audit program before receiving notification of selection for the HIPAA audit, please indicate how you heard about the audit program.

❍ Before receiving notice of selection for the HIPAA audit

❍ Upon receiving notice of selection for the HIPAA audit

3. Please indicate the time period during which the following events occurred at your organization/practice (select all that apply).

	At any time before receiving notice	Upon receiving notice	Between receiving notice and before on-site visit	During on-site visit	After on-site visit and before receiving audit report	N/A or Never
Became aware that the audit protocol was publicly available on the OCR website	❍	❍	❍	❍	❍	❍
Performed research on the HIPAA audit protocol or what would be required during an audit	❍	❍	❍	❍	❍	❍
Implemented a program to improve your HIPAA compliance	❍	❍	❍	❍	❍	❍
Conducted an internal HIPAA-related review (e.g. compliance department review or internal audit)	❍	❍	❍	❍	❍	❍
Participated in other, third-party HIPAA-related reviews (e.g. a certification program or another external audit)	❍	❍	❍	❍	❍	❍

3a. In what types of other, third-party HIPAA-related reviews did you participate? Select all that apply. Please indicate the agency or organization that conducted the review.

***Skip logic**: Only asked if response other than "NA" or "Never" is selected for the last statement of question 3.*

❍ Review for accreditation or certification by

❍ Review due to regulatory or other government program requirements

❍ Other review by

3b. Please indicate by area how the OCR audit compared in scope to the other HIPAA-related review(s).

***Skip logic**: Only asked if response other than "NA" or "Never" is selected for the last statement of question 3.*

	OCR audit narrower in scope	OCR audit similar in scope	OCR audit broader in scope	N/A
Privacy	❍	❍	❍	❍
Security	❍	❍	❍	❍
Breach Notification	❍	❍	❍	❍

The following questions relate to the communications sent and the materials requested prior to and during the on-site visit by the HIPAA auditors.

4. Please indicate the level to which you agree with each of the following statements.

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
Communications received prior to the on-site visit by the auditors clearly explained the purpose of the audit.	❍	❍	❍	❍	❍	❍
Communications received prior to the on-site visit by the auditors clearly explained what would happen during the audit.	❍	❍	❍	❍	❍	❍
Communications received *prior to* the on-site visit by the auditors clearly outlined the documents and data that were being requested.	❍	❍	❍	❍	❍	❍
Communications received *during* the on-site visit by the auditors clearly outlined the documents and data that were being requested.	❍	❍	❍	❍	❍	❍
Documents and data requested were sufficient for assessing HIPAA compliance for our type of entity.	❍	❍	❍	❍	❍	❍

5. Please comment on any aspects of the document and data request that made it easy for you to produce the requested materials.

6. Please comment on any aspects of the document and data request that made it difficult for you to produce the requested materials.

Page 4 – Audit Report

The following questions relate to the audit report.

7. Please indicate the level to which you agree with each of the following statements regarding the audit report that you received.

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
The report was clear and easy to read.	❍	❍	❍	❍	❍	❍
The report clearly identified gaps between the HIPAA requirements and our operations at the initiation of the audit process.	❍	❍	❍	❍	❍	❍
The report accurately described the state of HIPAA compliance at our organization at the initiation of the audit process.	❍	❍	❍	❍	❍	❍
The report provided an actionable basis for bringing our organization into HIPAA compliance (if there were no findings or observations in the audit report then select “N/A”).	❍	❍	❍	❍	❍	❍

8. Please suggest changes to the report that would have clarified the actions your organization needed to take to remediate audit findings.

Page 5 – Effect on Covered Entity

The following questions relate to the effect of the OCR HIPAA audit on your entity.

9. Please estimate the number of employee hours your organization spent to respond to the HIPAA audit.

10. Please provide a brief description of how you arrived at the hours estimate in question 9.

11. Please describe the alterations required in your organization's day-to-day business activities in order to accommodate the requests of the auditors.

12. Recognizing the necessity of the audits, please suggest changes to improve the HIPAA audit process.

Page 6 – Benefits to Covered Entity

13. Please indicate if the following statements apply to your organization.

	Applies		
	Yes	No	N/A
As a result of the OCR HIPAA audit, we became aware of additional HIPAA requirements that apply to our organization.	❍	❍	❍
As a result of the OCR HIPAA audit, we developed a plan to bring our organization into HIPAA compliance.	❍	❍	❍
We have improved our HIPAA compliance by addressing specific findings and/or observations in the audit report. If there were no findings or observations in the audit report then select N/A.	❍	❍	❍
As a result of the OCR HIPAA audit, we have improved our HIPAA compliance in areas other than those identified in the audit report.	❍	❍	❍

13a. You have indicated that the following statements apply to your organization as a result of the OCR HIPAA audit. Please indicate to which audit area(s) the statement applies.

***Skip logic**: Overall question only asked if "Yes" is selected for at least one of the statements in question 13. Statements only appear if "Yes" was selected for the corresponding statement in question 13.*

	Area			
	All	Privacy	Security	Breach Notification
We became aware of additional HIPAA requirements that apply to our organization.	❑	❑	❑	❑
We developed a plan to bring our organization into HIPAA compliance.	❑	❑	❑	❑
We have improved our HIPAA compliance by addressing specific findings and/or observations in the audit report.	❑	❑	❑	❑
We have improved our HIPAA compliance in areas other than those identified in the audit report.	❑	❑	❑	❑

13b. Please describe the aspects of the audit program that aided in developing a plan to bring your organization into HIPAA compliance.

***Skip logic**: Only asked if "Yes" is selected for the second statement of question 13.*

14. Please provide any other comments about the OCR HIPAA audit.