**From:** OSOCRAudit@hhs.gov [mailto:OSOCRAudit@hhs.gov]
**Sent:** Friday, May 20, 2016 3:38 PM
**To:** [redacted]
**Subject:** [BULK] OCR HIPAA Audit - Entity Screening Questionnaire

DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF THE SECRETARY

Voice - (800) 368-1019
TDD - (202) 619-2357
FAX - (202) 619-3818
http://www.hhs.gov/ocr

Director
Office for Civil Rights
200 Independence Ave., SW;
RM 509F
Washington, DC 20201

05/20/2016

[redacted]

Dear [redacted]:

The Office for Civil Rights (OCR) has responsibility for administration and enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules ("the Rules") (45 CFR Part 160 and Part 164 Subparts C, D and E). These Rules are designed to provide important health information privacy and security protections and rights for individuals. Through the American Recovery and Reinvestment Act of 2009 (ARRA), Congress required the Department to audit covered entity and business associate compliance with the HIPAA Rules. Audits present an opportunity for OCR to examine mechanisms for compliance; identify promising practices for protecting the privacy and security of health information; discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews; and better target the technical assistance it provides to covered entities and business associates.

Screening Questionnaire
You are receiving this notice because you have been selected to complete the pre-audit screening questionnaire linked below. This screening questionnaire is intended to gather data about the size, types, and operations of potential auditees for the HIPAA Privacy, Security and Breach Notification Audit Program. These data will be used with other information to help us select entities that reflect a variety of types, sizes, and locations for the next phase of the Audit Program. Receiving this notice does not mean your organization has been selected for an audit; rather, your organization is part of a pool from which OCR will select the entities that will be audited this year.

Please complete the screening questionnaire by providing the requested information. After checking the appropriate boxes to indicate your entity type, please respond to the referenced questions. Answer questions to the best of your knowledge. Data will be kept private to the extent allowed by law.

You have 30 days, until June 19, 2016, to complete this on-line screening questionnaire. If you do not respond to the questionnaire, we will use publicly available information about your organization to move forward with our audit program; failure to respond will not shield your organization from being selected for an audit or from becoming the subject of a compliance review. Please note that if your organization is selected for audit, communications from OCR will be sent to the email addresses of the contact person(s) you identify through the questionnaire.

You may submit questions regarding the questionnaire to OSOCRAudit@hhs.gov.

Click HERE to access the questionnaire.

The questionnaire must be completed and submitted online through our secure portal. You will be asked to respond to questions related to your size, entity type, services and best contact information. The questionnaire is available on our website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/questionnaire/index.html for preparation purposes only; please make all responses through the secure online portal using the link to the questionnaire provided above.

Selected Entities-Preparation for Documentation Submission
Covered entities and business associates will be notified of their selection for an audit on a rolling basis. Please be aware that if your entity is selected for an audit, you will have ten (10) business days to respond with the requested documentation. Among other items, selected entities must submit a list of all current business associates, with up to date contact information, within the 10 day response period. OCR will use this information to compile a list of potential business associate subjects to audit. OCR encourages entities to develop the business associate listing in advance to be able to meet the submission requirements. The business associate listing should be submitted as a spreadsheet with columns that contain the name of the entity, type of service(s) provided, primary and secondary contact names, titles, emails, phone numbers, address, website, if any. A template for the spreadsheet is available on our website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html.

Breadth of Audit and Audit Protocol
If you are selected for an audit, OCR will either; 1) conduct a focused desk audit to review documentation of evidence of your compliance with selected provisions of the Rules; or 2) conduct a comprehensive on-site review of your compliance with applicable requirements of the HIPAA Rules, or 3) follow up a desk audit with an onsite audit. The audit protocols, which contain criteria the auditors will use, will be available here: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html. OCR will assess whether to open a separate compliance review in cases where an audit indicates serious

compliance issues or where a covered entity or business associate fails to cooperate with an audit.

FOIA
Under the Freedom of Information Act (FOIA), OCR may be required to release audit notification letters and other information about these audits upon request by the public. In the event OCR receives such a request, we will abide by the FOIA regulations.

Sincerely,

Jocelyn Samuels
Director
Office for Civil Rights
OFFICE OF THE SECRETARY
Department of Health and Human Services
http://www.hhs.gov/ocr