

November 28, 2016

Alert: Phishing Email Disguised as Official OCR Audit Communication

OCR has posted the following information to our website:

It has come to our attention that a phishing email is being circulated on mock HHS Departmental letterhead under the signature of OCR's Director, Jocelyn Samuels. This email appears to be an official government communication, and targets employees of HIPAA covered entities and their business associates. The email prompts recipients to click a link regarding possible inclusion in the HIPAA Privacy, Security, and Breach Rules Audit Program. The link directs individuals to a non-governmental website marketing a firm's cybersecurity services. In no way is this firm associated with the U.S. Department of Health and Human Services or the Office for Civil Rights. We take the unauthorized use of this material by this firm very seriously.

OCR would like to further share that this phishing email originates from the email address OSOCRAudit@hhs-gov.us and directs individuals to a URL at <http://www.hhs-gov.us>. This is a subtle difference from the official email address for our HIPAA audit program, OSOCRAudit@hhs.gov, but such subtlety is typical in phishing scams.

Covered entities and business associates should alert their employees of this issue and take note that official communications regarding the HIPAA audit program are sent to selected auditees from the email address OSOCRAudit@hhs.gov. In the event that you or your organization has a question as to whether it has received an official communication from our agency regarding a HIPAA audit, please contact us via email at OSOCRAudit@hhs.gov.