

**Margaret Scavotto**

---

**From:** OCR HIPAA Privacy Rule information distribution <OCR-PRIVACY-LIST@LIST.NIH.GOV>  
on behalf of OS OCR PrivacyList, OCR (HHS/OS) <OCRPrivacyList@HHS.GOV>  
**Sent:** Thursday, August 6, 2020 1:35 PM  
**To:** OCR-PRIVACY-LIST@LIST.NIH.GOV  
**Subject:** Alert: Postcard Disguised as Official OCR Communication

**NOTICE: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.**

---

## HHS Office for Civil Rights in Action



---

### **Alert: Postcard Disguised as Official OCR Communication August 6, 2020**

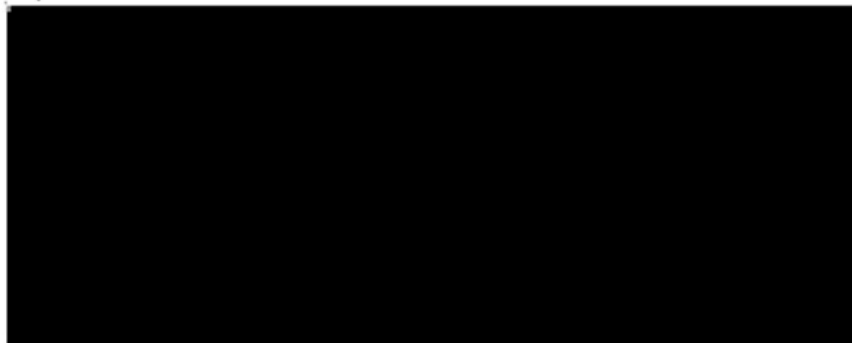
OCR has been made aware of postcards being sent to health care organizations disguised as official OCR communications, claiming to be notices of a mandatory HIPAA compliance risk assessment. The postcards have a Washington, D.C. return address, and the sender uses the title “Secretary of Compliance, HIPAA Compliance Division.” The postcard is addressed to the health care organization’s HIPAA compliance officer and prompts recipients to visit a URL, call, or email to take immediate action on a HIPAA Risk Assessment. The link directs individuals to a non-governmental website marketing consulting services.

**The postcard below is not from HHS/OCR.**

Secretary of Compliance  
HIPAA Compliance Division  
1032 15<sup>th</sup> ST  
Washington, DC 20005  
**ATTN: HIPAA COMPLIANCE OFFICER**



**Required Security  
Risk Assessment:**  
Per 164.308(a)(1) –  
**MANDATORY  
COMPLIANCE HIPAA  
ENTITY**



**NOTICE:** HIPAA violations cost your practice. The federal fines for noncompliance are based on the level of perceived negligence found within your organization at the time of the HIPAA violation. These fines can range from \$100 to \$50,000 per violation (or per record), with a maximum penalty of \$1.5 million per year for each violation. **See Reverse for Instructions**

HIPAA covered entities and business associates should alert their workforce members to this misleading communication. This communication is from a private entity – it is **NOT** an HHS/OCR communication. Covered entities and business associates can verify that a communication is from OCR by looking for the OCR address or email address on any communication that purports to be from OCR. The addresses for OCR's HQ and Regional Offices are available on the OCR website at <https://www.hhs.gov/ocr/about-us/contact-us/index.html>, and all OCR email addresses will end in [@hhs.gov](mailto:@hhs.gov). If organizations have additional questions or concerns, please send an email to: [OCRMail@hhs.gov](mailto:OCRMail@hhs.gov).

Suspected incidents of individuals posing as federal law enforcement should be reported to the Federal Bureau of Investigation.

###

---

\_\_\_\_\_ This email is being sent to you from the OCR-Privacy-List listserv, operated by the Office for Civil Rights (OCR) in the US Department of Health and Human Services. This is an announce-only list, a resource to distribute information about the HIPAA Privacy and Security Rules. For additional information on a wide range of topics about the Privacy and Security Rules, please visit the OCR Privacy website at <http://www.hhs.gov/ocr/privacy/index.html>. You can also call the OCR Privacy toll-free phone line at (866) 627-7748. Information about OCR's civil rights authorities and responsibilities can be found on the OCR home page at <http://www.hhs.gov/ocr/office/index.html>. If you believe that a person or organization covered by the Privacy and Security Rules (a "covered entity") violated your health information privacy rights or otherwise violated the Privacy or Security Rules, you may file a complaint with OCR. For additional information about how to file a complaint, visit OCR's web page on filing complaints at <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>. To subscribe to or unsubscribe from the list serv, go to <https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-PRIVACY-LIST&A=1>.