



THREAT BULLETINS

Misleading Postcard Disguised as Official OCR Communication



TLP:WHITE

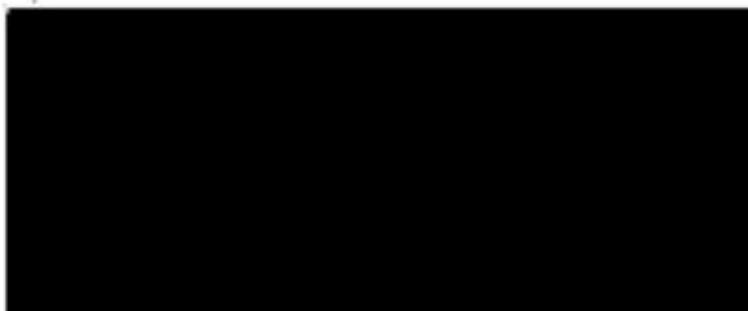
Apr 26, 2021

On April 26, 2021, HHS Office for Civil Rights in Action (OCR) was made aware of postcards being sent to healthcare organizations advising recipients that they are required to participate in a “Required Security Risk Assessment” which can be completed at [www\[.\]hsaudit.org](http://www[.]hsaudit.org). The link directs individuals to a non-governmental website marketing consulting services.

Secretary of Compliance
HIPAA Compliance Division
1032 15th 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**

Please be advised that these postcard notifications did not come from OCR or the US Department of Health and Human Services. The misleading communication is from a private entity – it is NOT an HHS/OCR communication.

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

Analysis:

HIPAA covered entities and business associates should alert their workforce members to this misleading communication. Covered entities and business associates can verify that a communication is from OCR by looking for the OCR address or email address, which will end in @hhs.gov, on any communication that purports to be from OCR, and asking for a confirming email from the OCR investigator's hhs.gov email address.

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.

If organizations have additional questions or concerns, please send an email to: OCRMail@hhs.gov.

Info Source

Intel Agency (FBI, NSA, etc.)

Sources

[Misleading HIPAA Postcard Warning](#)

[Postcard Disguised as Official OCR Communication](#)

[Alert: Fake Postcard Disguised as OCR Communication](#)

[OCR warns hospitals of HIPAA compliance scams](#)

[OCR Warns of Postal Scam Targeting HIPAA Compliance Officers](#)

Alert ID d534f704

[View Alert](#)

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.



For more update and alerts, visit: <https://health-isac.cyware.com>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.

Powered by [Cyware](#)