Published on *The National Law Review* https://natlawreview.com

Beware, Persons Posing as OCR Investigators Demand PHI, Says OCR Alert

Article By:

Joseph J. Lazzarotti

On April 3, the Office for Civil Rights (OCR) issued an alert to covered entities and business associates. Evidently, one or more individuals are posing as OCR Investigators and contacting HIPAA covered entities and business associates in an attempt to obtain protected health information (PHI). The individual identifies on the telephone as an OCR investigator, but does not provide an OCR complaint transaction number or any other verifiable information relating to an OCR investigation. In this environment, with many healthcare providers stretched to their limits dealing with COVID-19, workforce members may be distracted, fail to follow normal protocols, and simply comply with the request.

Verification should be a regular step, second-nature, in the process of making disclosures of PHI. The basic rule at 45 CFR 164.514(h) provides that, in general

> *Prior to any disclosure permitted by this subpart, a covered entity must:*
>
> *(i) … verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and*
>
> *(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.*

OCR recommends HIPAA covered entities and business associates should alert their workforce members of these potential scams, and remind them of the basic verification requirement. They also should provide some easy to follow tips for verification, such as:

- Do not provide any PHI information based solely on a telephone request until verified.
- Ask for the name and transaction number for the matter the caller is calling about.
- Ask for the caller to provide his or her email address, it should end in @hhs.gov.

- Ask the caller’s name, title, and what OCR office they are calling from.
- Ask for an email from the OCR investigator confirming the nature and scope of the request.
- Ask the caller if he or she has communicated with anyone else at the organization about the matter.
- Ask for a copy of any prior written request(s) for the information, there usually is one.
- Remind workforce members about best practices for responding to phishing and spoofing attacks.

Covered entities and business associates might also centralize the function of responding to such requests to one person, a small group of workforce members, or a third party. Typically, that person, group, or third party is better trained to follow these and other best practices for verification.

Organizations with additional questions or concerns, or that may be questioning a particular inquiry, could reach out to the OCR at: OCRMail@hhs.gov. The OCR also reminded covered entities about other COVID schemes and that suspected incidents of individuals posing as federal law enforcement should be reported to the Federal Bureau of Investigation (FBI) at www.ic3.gov.

National Law Review, Volume X, Number 96