

# PUBLICATION

---

## Medical Records Scams: What You Need to Know

Authors: Alisa L. Chestler

June 21, 2024

In today's digital age, the health care industry faces a growing threat from scammers who don't have to use sophisticated cyberattacks; they can use the most routine task to steal information from unwitting and well-intentioned employees. All covered entities, providers, health plans, and their business associate partners must be aware of the latest scam directed at medical records departments. In the June 20, 2024, release of the *mInconnects*, issued by the Centers for Medicare & Medicaid Services (CMS), CMS puts the community on notice of the latest scam.

CMS has apparently identified a scam in which medical records requests are faxed to providers asking for medical records. The example provided can be viewed here: <https://www.cms.gov/files/document/medical-record-phishing.pdf>

When considering whether a request is a scam, CMS provided the following tips:

- Does the request direct you to send records to an unfamiliar fax number or address;
- Does the request reference Medicare.gov or @Medicare (.gov); or
- Does the request indicate they need records to "update insurance accordingly."

CMS noted that scams may also be spotted through identification of the following:

- Poor grammar, misspellings, or strange wording;
- Incorrect phone numbers;
- Skewed or outdated logos; or
- Graphics that are cut and pasted.

All providers, health plans, and their vendors must exercise diligence in verifying the authenticity of requests for medical records or services. By adopting verification protocols the risk of falling prey to a scam can be mitigated. If you have questions about how to protect against medical record scams, please reach out to [Alisa L. Chestler](#) or any member of Baker Donelson's [Data Protection, Privacy and Cybersecurity Group](#).