Codify
BY AAPC

# Health Information Compliance Alert

## Reader Questions: Safeguard ePHI from Unauthorized Disclosure With This Advice

**Question:** A provider in our practice informed us that they have been sending patient records to their personal email to review at home. Does this constitute an unauthorized disclosure of electronic protected health information (ePHI), and does it pose a security risk?

Ohio Subscriber

**Answer:** Yes, the provider's actions can constitute an unauthorized disclosure of ePHI and pose a security risk.

Unauthorized disclosure of health data can be just as dangerous to a patient's privacy as a ransomware attack. While the latter garners more attention from health IT pundits, the media, and the feds, unauthorized access or disclosure of ePHI is just as serious.

Some unauthorized disclosure incidents may be malicious in their intent, but most incidents, such as the one you're describing, are due to negligence or improper cybersecurity education. People in the system, such as doctors and clinicians, may just want to access the patient's information and medical record to deliver treatment but are violating disclosure rules.

When patients arrive at your practice, you're committed to protecting their ePHI. Once the patients' records leave your practice's network, there's no way to ensure that protection and that could cause major headaches if the provider's personal device or accounts become targets of cybercriminals.

By educating your employees on the safe handling of ePHI and proper cyber hygiene techniques, your practice or facility can help prevent incidents of unauthorized disclosure.

Codify
BY AAPC