Report on Medicare Compliance Volume 27, Number 43. December 10, 2018

In Phishing Epidemic, Debate Rages Over Whether to Discipline Employees the Usual Way

By Nina Youngstrom

In early 2018, a worried employee of ATI Physical Therapy in Bolingbrook, Illinois, told Chief Compliance Officer Lynn McGivern there was no paycheck in the employee's bank account. ATI's internal investigation immediately discovered that hackers embezzled $40,000. They had used a phishing email to trick the employee to change her password in the human resources system so direct-deposit paychecks could be redirected to offshore accounts. ATI notified patients in case their data was compromised, although McGivern doubts it, and the HHS Office for Civil Rights did a compliance review, but the results aren't in. The phishing and its aftermath have led to significant changes: For example, ATI blocks all links coming in until their provenance is confirmed. "It was an ordeal," she says.

What happened to the employee who inadvertently opened the virtual door to cybercriminals? "We did not discipline the individual we knew clicked on the link," McGivern says. Partly she was duped because the phishing email used the name of a person in the organization, and it's hard to tell it's a fake without looking very closely. "It was an unfortunate event," McGivern says. Even ATI's board of directors said, "This stuff is going to happen."

There is no consensus in the health care industry about discipline for employees and others who succumb to phishing emails, says Alexander Laham, information security manager at Lawrence General Hospital in Massachusetts. Like the thousands of health care organizations across the country whose employees give hackers the keys to the kingdom by clicking on links in a phishing email, they are debating whether to discipline employees the same way they would for any other mistake/misconduct, experts say. Whatever organizations decide about discipline, their education should penetrate minds and hearts because hackers pose a grave threat to the privacy, security and finances of health care organizations, compliance experts say. Teach context clues—for example, think twice before opening an email from the CEO if you've never before received one from him or her—and maybe only discipline employees who repeatedly open phishing emails despite education.