Children's of Alabama Compliance Corner

Costly Data Breach at Anthem

Recently, the nation's second largest insurer, Anthem, agreed to pay a $16 million settlement to the U.S. Department of Health and Human Services for HIPAA violations after several cyberattacks called "phishing emails" were sent to its employees. This breach, dating back to 2014, exposed the electronic Personally Identifiable Information (PII) of almost 79 million Anthem consumers. We interviewed Paul Cofer, in COA's IT department, to learn how this happened and how we can prevent it from happening here.

Paul, what events led up to this data breach?

A combination of gaps in security awareness training, cyber security controls, and privilege access management allowed this breach to happen. The attackers who "hacked in" were in the Anthem network for 11 months before detection, gained access to 50 accounts, and broke into 90 different computer systems. Had tools been in place to identify network weaknesses and unauthorized download of Anthem's data, the extent of the breach wouldn't have been what it is today.

What can our employees learn from this experience?

Employees should

- Carefully examine the "From" address of the sender
- Be aware of scare tactics used in social engineering attacks, such as "Your mailbox is full, click here to login to avoid disruption"
- Hover the curser over links in the email to reveal the true destination
- When in doubt, ask! Contact the Customer Support Desk (638-6568) or, if using Outlook, click on the "Phishing Alert Report Email" button in the top portion of your inbox's task bar.

Children's has made significant investments in cyber security tools to help protect our databases from these types of incidents; however, user awareness is the greatest prevention against phishing.

*Reference – *Electronic Mail Policy* in Lucidoc