FOR IMMEDIATE RELEASE
December 3rd, 2019

Media Contact:
John E. Thomas
Healthcare Administrative Partners, LLC
610-892-8889
JThomas@hapusa.com

Healthcare Administrative Partners Provides Notice of Data Security Incident

MEDIA, PA. December 3rd, 2019. Healthcare Administrative Partners ("HAP"), a provider of billing services to health care providers, recently notified Radiology Group of Abington ("RGA") of a data security incident affecting RGA and its affiliates, Abington PET/CT of Willow Grove, Fort Washington Radiological Associates and the Vein Institute of Blue Bell. The data security incident arose from a phishing attack that resulted in an unauthorized individual gaining access to the email account of a HAP employee. Out of an abundance of caution, RGA and HAP are notifying potentially impacted individuals as well as regulators of the incident.

What happened? On October 4, 2019, HAP notified RGA that it had experienced a data security incident. As part of its investigation, HAP engaged independent computer forensic experts, which determined that an unauthorized individual accessed an employee's email account through a phishing attack. Unfortunately, forensics was unable to identify what emails or attachments, if any, may have been viewed by the unauthorized individual. Because HAP was unable to make this determination, they conducted a thorough review of the mailbox contents to identify what personal or protected health information may have been present in the email account.

What Information Was Involved? On September 16, 2019, HAP learned that the email account contained patient information provided to HAP for billing purposes, which may have included some combination of patient name, date of birth, healthcare provider, medical record number, CPT or diagnosis code, and limited treatment information.

What HAP is Doing: HAP has taken numerous steps to prevent this kind of event from happening in the future. Since the incident, all passwords have been reset, external emails are now clearly labeled as external, mailbox size restrictions and archiving requirements have been implemented, and HAP is evaluating options for multi-factor authentication. HAP employees are also being retrained on recognizing and responding to suspicious emails.

For More Information: Individuals seeking more information about this incident may call 1-833-281-4831 Monday through Friday from 9 am – 11 pm Eastern Time, Saturday/Sunday 11 am -8 pm Eastern Time with questions.

What You Can Do: While HAP believes misuse of any patient information is unlikely, they encourage patients to review their explanation of benefits and immediately contact their provider if they identify suspicious activity. Individuals can also contact the Federal Trade Commission at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261 or visit www.ftc.gov/idtheft/ for more information on protecting their identity.