Notice of a Data Security Incident

First Physicians Business Solutions LLC ("First Physicians") is committed to protecting the security and confidentiality of the information we maintain. This notice describes an incident that may have involved information pertaining to patients of Stroud Regional Medical Center ("Stroud"). First Physicians provides administrative and technology services to Stroud.

On February 26, 2021, we identified unusual activity within an email account used by a Stroud contractor employed by First Physicians. We immediately took measures to secure the email account and launched an investigation with the assistance of a cybersecurity firm. The investigation determined that the contractor's email account was subject to unauthorized access on February 26, 2021. Although we did not find any evidence that emails or attachments were actually viewed, we could not definitively rule out that possibility. Based on the activity that took place within the account on February 26, we identified emails and attachments that were at risk of being viewed by the unauthorized person and reviewed those emails and attachments to determine what, if any, personal information they contained. On June 4, 2021, we determined that some of these emails or attachments contained information related to a limited number of Stroud patients, including patients' names, dates of birth, Social Security numbers, and diagnosis and/or treatment information. On July 12, 2021, we notified Stroud of the incident.

On August 2, 2021, we mailed letters to patients whose information was identified in the relevant emails and attachments. We are offering patients whose Social Security numbers were identified in those emails/attachments complimentary credit monitoring and identity theft protection services. If patients have questions about this incident, please call 866-991-0830, Monday through Friday, between 8:00 a.m. and 8:00 p.m., Central Time.

We recommend that patients whose information may have been involved in this incident review the statements they receive from their healthcare providers. If they see any services that were not received, they should contact the provider immediately.

We deeply regret any concern this may cause. To help prevent something like this from happening in the future, we are reinforcing education of our workforce on how to identify and avoid phishing emails and have implemented multi-factor authentication for our email environment.