



October 22, 2020

Notice of Recent Email Incident

Perry County Memorial Hospital (“PCMH”) is hereby notifying individuals of an email incident that resulted in unauthorized access to two email boxes that was blocked on or about August 23, 2020. These email boxes may have contained personal information for some individuals.

Fortunately, the incident was limited to only two employee email accounts and did NOT affect PCMH’s overall medical / billing / human resources records systems. Also, PCMH has NOT received any report of identity theft as the result of this incident.

PCMH promptly responded to this incident — changing passwords to block suspicious activity and unauthorized access. In an abundance of caution, outside technical experts were retained to help with investigating the incident in order to evaluate the full nature and scope of any potential access to ensure there was no access to individual personal information.

On September 10, 2020, we were alerted by these experts that, because of the method of access, one email account may have been at risk of being copied — likely inadvertently during the standard email synchronization process.

We then conducted an extensive document review process to determine whether individual names or other sensitive data were located within any of the emails that may have been affected.

We are in the process of sending a notification letter to the individuals (for whom we have a mailing address) where we determined that personal information was potentially involved.

To date, it appears the information potentially involved was full name, date of birth, diagnoses/diagnostic codes, internal patient account numbers, provider names, and other health information. In a limited number of instances, social security numbers, Medicare/Medicaid numbers, and health insurance information may have been in the affected email accounts.

PCMH values the safety and security of the data that it maintains and is continuing to take steps to enhance its security measures to help prevent something like this from happening in the future.

While we have no evidence that any personal information has actually been used inappropriately, we recommend affected persons remain vigilant and monitor financial account statements and credit reports carefully and report discrepancies to law enforcement. Fraud alerts and security freezes also can be activated to help protect individuals. PCMH is providing identity theft monitoring to any individual whose social security number was potentially within the email accounts.

PCMH is setting up a toll-free call center to answer questions, which will be available for 90 days starting on **October 22, 2020**. If you are concerned your information was involved in this incident, please call 888-768-6008 Monday through Friday from 9 a.m. to 4:00 p.m. CST, excluding holidays, to verify and obtain additional information regarding whether your information was potentially affected.