

CYBERSECURITY INFORMATION

Please read below for an updated statement from COPC regarding a recent cybersecurity incident. A version of this was distributed to appropriate media outlets.

Updated 10/15/26

Central Ohio Primary Care Physicians, Inc. (“COPC”) has identified and responded to a cybersecurity incident that may have exposed the personal information of its patients and employees.

On August 25, 2026, COPC discovered that it had experienced a cybersecurity incident resulting from a social-engineering, or “vishing” (voice phishing), attack, carried out in an attempt to solicit a financial response. Through this attack, a criminal threat actor was able to gain unauthorized access to certain files containing protected health information.

Upon detection, COPC engaged cybersecurity experts to assess and contain the incident. The organization has since been working closely with authorities and cybersecurity professionals to assess exposure, reinforce security measures and focus on preventing future incidents.

To note, this incident has been contained with no further unauthorized access in our systems. MyChart (Epic) was not impacted by this incident, and patients can continue to log into the portal and connect with their provider as usual.

To date, COPC is unaware of any misuse (or attempted misuse) of personal information for identity theft or fraud stemming from the Incident. The information potentially exposed may have included protected health information, which could include sensitive personal information such as first and last name, address, Social Security Number, limited health related patient data including patient ID number, financial information, and other potential identifying information.

While the full extent of the incident is still under review, our initial investigation discovered that there are approximately 1.4 million individuals impacted. COPC is committed to supporting those individuals in accordance with both its internal regulations as well as applicable law.

COPC is helping potentially exposed parties by providing complimentary credit and dark web monitoring services through IDX Identity Theft Protection Plan. In addition, the COPC internal teams are continuing to work with third-party experts to follow best practices as well as federal and state regulations intended to protect those individuals who are exposed in these types of incidents.

Impacted individuals with contact information on file with COPC will receive written notification. All others who believe they may be impacted as patients of COPC and do not receive a letter may go to <https://response.idx.us/copc> for more information, to request confirmation of impact, and to request a credit monitoring sign-up code.

The letter and the website provide details regarding the steps they can take to safeguard their information, including instructions for signing up for IDX credit monitoring and placing security freezes on their credit profiles. **COPC has also established a dedicated call center to address concerns and provide additional support to those impacted. The call center number is 1-866-200-0918 and is open Monday through Friday, 9 AM – 9 PM.**