

Henry Ford Health is notifying some of their patients that an unauthorized individual conducted an email phishing scheme to gain access to business email accounts. The improper access was quickly discovered and the email accounts were secured.

Here are important facts to know:

- Some of patient information was contained in the affected email boxes, but we don't know whether such information was actually accessed or not.
- Phishing email schemes are used to fraudulently obtain victims' credentials or personal information by sending them fake email messages.

The incident occurred on March 30, 2023 and we immediately began an extensive investigation to determine what happened.

Through our forensics investigation, we determined on May 16, 2023 that protected health information was contained in the email boxes and could have been accessed by the bad actor.

The information stored on the affected email accounts may have included the following: name, gender, date of birth, age, lab results, procedure type, diagnosis, date of service, telephone number, medical record number and/or internal tracking number.

As a result of this incident, we are implementing additional security measures and providing additional training to employees about recognizing the signs of suspicious email and what to do if they receive one.

If there are questions, please call our Incident Response Line at **833-627-2685 between 9 a.m. and 9 p.m. Eastern Time, Monday - Friday**. That number goes to our business partner, Epiq Solutions, a call center based in Portland, Oregon that specializes in providing assistance for data security and cybersecurity incidents and services for other industries.