A Notice to Our Patients

Atrium Health is committed to protecting the confidentiality and security of our patients' information. Regrettably, we recently identified a security incident that may have involved some of that information.

On or about April 29, 2024, we learned that an unauthorized third party gained access to some employee email accounts on that same day through "phishing." Phishing occurs when an email looks like it is from a trustworthy source, but is not. The malicious email misleads the recipient into sharing or providing access to their account login information.

We immediately began an investigation, took the necessary steps to secure the affected accounts and confirmed the unauthorized third party had no further access. We also engaged a forensic consultant to assist with the investigation and notified law enforcement. Based on our findings, it appears the unauthorized third party may have had access to the affected accounts for a short time from April 29-30. We confirmed the unauthorized third party did not access Atrium Health's electronic health record systems. The forensic consultant's analysis of the affected accounts, completed on July 17, 2024, indicates that the unauthorized party was not focused on email content pertaining to medical or health information.

Unfortunately, it was not possible to conclusively determine whether the third party actually viewed any emails or attachments contained in the affected accounts. As a result, with the assistance of the forensic consultant, we conducted a review of the accounts to determine what information may have been accessible to the party. This information may have included one or more of the following: an individual's first and/or last name; middle initial; street address, email address and/or phone number(s); Social Security number; date of birth; medical record number; certain government or employer identifiers; driver's license or state-issued identification number; bank or financial account numbers or information, including routing numbers, financial institution name, or expiration date; treatment/diagnosis, provider name, prescription, health insurance or treatment cost information; patient identification number; health insurance account or policy number(s); incidental health references; billing identification numbers; access credentials; and/or digital signatures.

Not all of Atrium Health's patients were impacted, only those whose information happened to be in the files used by the affected employees' accounts. Additionally, our electronic medical record systems are separate from our email accounts and were **not** affected by this incident.

We have no indication that anyone's information was actually viewed by the unauthorized third party or that it has been misused. However, as a precaution, we are mailing notification letters to people whose information was identified through our review and for whom we have sufficient contact information. The notification letters include a reference guide that provides additional information on general steps people can take to monitor and protect their personal information. Although we are unaware of any actual or attempted misuse of patient or personal information as a result of this incident, we encourage affected individuals to carefully review their credit reports and similar types of documents that might indicate questionable activity.

We have also established a dedicated toll-free call center to answer questions that people may have about the incident. If you have questions, please call (866) 997-1986, available Monday through Friday from 9 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

We apologize for any concern or inconvenience this incident may have caused and remain committed to protecting the confidentiality and security of our patients' information. We have and will continue to enhance our security controls, as appropriate, to minimize the risk of similar incidents in the future. We also continue to provide phishing and other cybersecurity training and education to our employees.

Frequently Asked Questions

1. **What happened?**

On or about April 29, 2024, an unauthorized third party used an email phishing campaign to gain access to some employee email accounts. Atrium Health became aware of this incident that same day on April 29, 2024, and immediately initiated an internal investigation, taking the necessary steps to secure the affected accounts and confirmed the unauthorized third party had no further access. We also engaged a forensic consultant to assist with the investigation and notified law enforcement. Based on our findings, it appears the unauthorized third party had access to the affected accounts for a short time between April 29-30. The forensic analysis indicates the activity of the unauthorized third party was not focused on email content pertaining to medical or health information.

2. **What personal information of mine may have been affected?**

This information may have included one or more of the following: an individual's first and/or last name; middle initial; street address, email address and/or phone number(s); Social Security number; date of birth; medical record number; certain government or employer identifiers; driver's license or state-issued identification number; bank or financial account numbers or information, including routing numbers, financial institution name, or expiration date; treatment/diagnosis, provider name, prescription, health insurance or treatment cost information; patient identification number; health insurance account or policy number(s); incidental health references; billing identification numbers; access credentials; and/or digital signatures.

3. **What have you done to keep something like this from happening again?**

We are committed to protecting the security and privacy of the information we maintain. At the time of this incident, Atrium Health already had security measures in place, including requiring annual privacy and security training of all employees. We continue to enhance our security controls, as appropriate, to minimize the risk of similar incidents in the future. We also continue to provide phishing training and education to our employees.

4. **Why does Atrium Health have my information?**

As a health system, we maintain the personal information of patients and their guarantors in our files, and maintain information pursuant to state and federal requirements. We have your information because you are a current or former patient of Atrium Health, or a guarantor of a current or former patient of Atrium Health.

5. **What can I do now?**

It is always a good idea to review the statements you receive from your healthcare provider and health insurer. If you see services that you did not receive, please contact the provider or insurer immediately. As a best practice, you can also review recommendations at the Federal Trade Commission's website, www.identitytheft.gov. You can obtain information from this website about steps you can take to help avoid identity theft as well as information about fraud alerts and security freezes.