Substitute Notice and Web FAQ

Saint Agnes Medical Center ("Saint Agnes") in Fresno is a proud member of Trinity Health, a multi-institutional Catholic health care delivery system, serving diverse communities that include more than 30 million people across 22 states.

On February 5, 2021, Saint Agnes was notified by its sister health system, Saint Alphonsus Health System ("Saint Alphonsus"), located in Idaho/Oregon, that an email account of a Saint Alphonsus employee had been compromised by an unauthorized user. This individual used the employee's email to send phishing emails, January 4-6, 2021, in an attempt to obtain login IDs and passwords.

The purpose of this notice is to inform you that the incident may impact the privacy of certain information related to you. This notice describes the immediate actions taken by Trinity Health, Saint Alphonsus and Saint Agnes to address the incident. It also gives you important details about the impact to you and how you can enroll in the free credit monitoring service we are offering you.

What happened
On February 5, 2021, Saint Alphonsus notified Saint Agnes that the email account of one of its colleagues had been accessed by an unauthorized user between January 4-6, 2021. This included a report with protected patient health information. Saint Alphonsus made the initial discovery on January 6, 2021 and moved quickly to identify the source and nature of the activity and to secure the email account to prevent future cyber-attacks.

Initially, the incident was thought to only affect Saint Alphonsus. It was later discovered that some of the compromised information from the report belonged to Saint Agnes patients because hospital billing for the West Region (that includes Saint Agnes) is handled by Saint Alphonsus. As soon as this detail came to light, Saint Agnes was notified.

What information may have been subject to unauthorized access?
Unfortunately, we have been unable to specifically determine what, if any, emails may have been viewed during this timeframe. While there is no evidence of any misuse of information in the email account, a thorough review of the contents of the account was conducted to determine what information might have been accessible at the time of this event. Through the review it was determined that a combination of the following types of information might have been accessible: patient’s full name, address, telephone, date of birth, email, and medical information such as medical record number, treatment information and billing information.

What actions did the health system take?
Trinity Health and Saint Agnes take these matters extremely seriously. Upon discovery of the incident Trinity Health immediately secured the employee’s email account to ensure the unauthorized individual could no longer access the account. We have no evidence of any misuse of the information within the email account.

We deeply regret any inconvenience or concern this situation may have caused you. We believe this to be an unfortunate and isolated incident. We want to assure you that Trinity Health and Saint Agnes are committed to protecting health information through significant investments in a strong security
program that includes a dedicated cybersecurity team, 24/7/365 monitoring, and testing of security controls.

What is available to affected patients?

Out of an abundance of caution, credit monitoring and an information call center will be offered to all affected patients. To ensure timely answers to your questions and concerns, please call 1-855-908-1274.

What do I need to do?

You do not need to take any action at this time. As always, you should remain vigilant and monitor your personal information to ensure it is not being used maliciously.