

Website Notice

Seneca Nation Health System Updated Notice of Data Security Incident

December 20, 2024 – Seneca Nation Health System is providing this updated notice of an incident involving potential unauthorized access to some individuals' information. Earlier this year, we detected a cybersecurity incident involving unauthorized activity on our systems. We promptly began investigating and responding to that incident, including posting notice of the incident on our website. We are now providing this updated notice to share more information on what happened and what we are doing in response.

WHAT HAPPENED

On April 30, 2024, we detected suspicious activity on our systems. We immediately took steps to secure our systems and began working with cybersecurity experts to assist us in the investigation. On May 10, 2024, we posted notice of the incident on our website. Based on the investigation, we believe that an unauthorized third party gained access to a portion of our computer systems from April 23 to 30, 2024, and that personal information was present in those affected systems. Once we identified the affected files, we promptly engaged a data-review firm to determine what information was contained in those files. We recently received the results of that review, and we have been working diligently since then to determine who needs notice.

WHAT INFORMATION WAS INVOLVED

The investigation determined that the following types of information were present in the affected files: full name, date of birth, contact information, government identification (such as a Social Security or driver's license number), health insurance information, patient identification number, date(s) of service, provider name(s), diagnosis, treatment information, prescription(s), medical history, radiology imaging and reports, medical consent forms, and lab reports. The categories of impacted information can vary considerably from individual to individual.

WHAT WE ARE DOING

Protecting the integrity of the information we maintain is a responsibility we take very seriously. We hired third-party experts to help us perform an investigation into the unauthorized activity and further secure our systems and the information we maintain. We also notified law enforcement. We previously shared details of this incident on our website, and we are now posting this updated notice and mailing notice to potentially affected individuals as required by law.

WHAT YOU CAN DO

For individuals who receive a letter from us about the incident, we encourage them to read the information in that letter carefully, as it contains important steps that they can take. We encourage individuals to (1) remain vigilant for unauthorized financial activity by reviewing their account statements and free credit reports, (2) consider placing a fraud alert or security freeze on their credit file (which individuals can do for free), and (3) immediately report any suspicious activity or suspected incidents of identity theft to their financial institutions and to law enforcement. Additional steps can also be found at www.IdentityTheft.gov/.

FOR MORE INFORMATION

We have established a toll-free call center to support impacted individuals and to answer their questions about the incident and this notice. The call center can be reached at (866) 573-9422.