Website Notice

ESO Solutions Provides Notice of Cybersecurity Incident

Notice of Cybersecurity Incident
We are committed to providing you with information about an incident that may have exposed certain protected health information and personal information related to the work we do with some of our customers. On the behalf of Trinity Medical Center West, ESO Solutions, Inc. ("ESO") provides software services that help hospitals and healthcare systems improve operations, quality, and patient outcomes. For this reason, ESO is likely to have certain individuals' information from when a healthcare organization provided injury or emergency care to them in the past. We take the security of information seriously and are providing notice and resources so potentially impacted individuals can protect themselves.

What Happened
On September 28, 2023, we detected and stopped a sophisticated ransomware incident, in which an unauthorized third party accessed and encrypted some of ESO's computer systems. We immediately took the affected systems offline, secured our network environment, and engaged third-party forensic specialists to assist us with investigating the extent of any unauthorized activity.

Our investigation determined that the unauthorized third party may have acquired some personal data during this incident. Please know that we have taken all reasonable steps to ensure the impacted data will not be further published or distributed, and have notified and are working with federal law enforcement to investigate.

While we have found no evidence that impacted information has been misused and taken steps to ensure data will not be further published or distributed, on October 23, 2023, we determined that some patient information was located on one of the impacted systems. As such, we are notifying impacted individuals of this incident via U.S. mail and offering them resources, in an abundance of caution and so that they can take precautionary steps to protect themselves, should they wish to do so. ESO recommends that individuals proceed with caution and take advantage of the resources provided in this letter.

What Information Was Involved
The impacted data varied by individual, but it may have contained personal information, including names, phone numbers, addresses, and some sensitive personal information and/or protected health information. Beginning on [date], we are mailing letters to affected individuals and while, to date, ESO is unaware of any misuse of the involved information, as a precaution, we are offering complimentary credit monitoring and identity theft protection services to individuals whose Personal Identifiable Information (PII) may have been impacted. Each notification letter sent to impacted individuals will include a list of specific data elements that were impacted as well as resources that they may use to protect themselves.
If you received a letter, your information was determined to be involved in this incident. We recommend you take advantage of the resources we are offering. If you do not receive a notification letter in the coming days, that means that we have not identified you as being someone whose sensitive data was impacted by this incident.

What We Are Doing
Data security is one of our highest priorities. Upon discovery of the incident, we immediately secured our networks, implemented measures to confirm the security of our systems, safely restored our systems and operations via viable backups, initiated an investigation of the incident with the assistance of forensic experts, and notified the FBI (Federal Bureau of Investigation).

We value the safety of your personal information and want to make sure impacted individuals have the information they need to take steps to further protect their information, should they feel it appropriate to do so. We encourage all individuals to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps below.

We have also secured the deletion of all impacted data and taken all reasonable steps to ensure the impacted data will not be further published or distributed.

What You Can Do
Again, to help relieve concerns following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to impacted individuals for <12/24> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

As previously shared, we recommend impacted individuals take advantage of the resources we are offering. For all individuals, however, it is always a good idea to remain vigilant by regularly monitoring your account statements and credit history for any signs of unauthorized transactions or activity.

For More Information
Representatives are available to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding holidays. Please call the help line at (866) 347-8525 with any questions you may have.

On behalf of ESO, please accept our sincere apology for this incident and any inconvenience it may cause you. We value the security of the protected health information and personal information that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused. We continue to build on our already substantial investments in cybersecurity to prevent an incident like this from reoccurring and protect the information entrusted to us now and in the future.