Notice of Security Incident

The Stern Cardiovascular Foundation, Inc. ("Stern Cardiovascular") is giving notice about a recent security incident that may have involved some patients' personal information.

On or about September 6, 2022, The Stern Cardiovascular Foundation, Inc. ("Stern Cardiovascular") experienced a data security incident that caused disruption to certain portions of our information technology network. We immediately investigated and aggressively responded to this incident. Passwords were changed, the unauthorized access was blocked, and law enforcement was notified. Outside technical experts were also engaged to further investigate and evaluate the nature and scope of the incident. Stern Cardiovascular's IT team has been working closely with these experts to remediate this event and to further harden Stern Cardiovascular's defenses.

During the course of its investigation, on September 13, Stern learned that unauthorized third part(ies) may have accessed or potentially exfiltrated certain limited files from its IT environment in connection with this incident on or around September 4 – 6. In response, Stern undertook an extensive document review process of the impacted files (which involved hand reviewing individual documents) to determine whether any sensitive information was contained in the files and to be able to identify individuals who potentially needed to be notified of this incident.

Although Stern currently has no evidence that its data has been misused, as potentially impacted individuals are identified, notification letters are being sent out of an abundance of caution via first class U.S. mail to the last known address of the individual or legal guardian. Stern also posted public notice of this incident on our website on November 6, 2022.

The information affected varies widely by individual and in some cases included name, address, date of birth, driver's license and/or state ID number, financial account number, payment card number, tax ID number, username and password, Insurance Information, date(s) of service, provider name(s), medical record number, patient number, diagnostic and/or treatment information, surgical information, medications, and/or other general medical information. For some individuals, the personal information involved included a Social Security number, and these individuals are being provided complimentary credit monitoring and identity theft protection services as required by law.

Persons potentially affected are encouraged to remain vigilant and monitor financial account statements and credit reports carefully and report any discrepancies to law enforcement. Additional guidance that individuals can take to protect themselves can be found at: https://www.consumer.ftc.gov/features/feature-0014-identity-theft

For more information about this incident and protective steps potentially affected persons may wish to take, individuals can call (888) 541-1931 between the hours of 8:00 am and 5:00 pm, Central Time, Monday - Friday (excluding major U.S. holidays). We are fully committed to protecting personal information and sincerely apologize for any concern this incident may have caused.