At First Step of Sarasota protecting the personal, clinical and medical information of our clients is one of our top priorities. Unfortunately, First Step was the victim of a security incident whereby a third party accessed personal health information (PHI) and / or personal identifying information (PII).

We are providing notice of a data incident that may affect the security of some information relating to a segment of our employee and patient population. Although we have no evidence that any client or employee personal information has been misused, we are providing information to make the public aware of the security incident so that anyone potentially effected may take any necessary precautions. We have provided individual notifications for potentially impacted parties but are providing this notice for anyone for whom we do not have a current mailing address. **If you have any additional questions, please call 833-375-4145.**

What Happened? Beginning at least as early as January 24, 2022, an intruder illegally gained entry to the FSOS computer network through a third-party. Cyber criminals used a ransomware attack to block accesses to servers. FSOS discovered the intrusion the same day, and promptly began the process of: working to contain the incident, notifying the FBI, engaging a third-party consultant to assist with containment, restoration, forensics, and notification. First Step has since continued to enhance security, monitor the situation and adhere to all requirements as it relates to this incident. FSOS has engaged experienced specialists to conduct an extensive analysis of the data to determine what was impacted.

What Information Was Involved? At this stage in this fluid situation, we know that some client and employee personal information was illegally accessed. However, there is no evidence the information was actually distributed or misused.

How did FSOS Respond? First Step takes the protection of personal and medical information on its network very seriously. We have enhanced our systems and security protections which will aid in the prevention and recurrence of similar incidents. First Step has taken immediate action to remove any system vulnerabilities, including changing relevant administrative passwords, installing security patches, and increasing tracking and monitoring of activity.

First Step has also retained the services of an experienced cyber security and forensic team. Based on our investigation to date, it is believed that only a limited amount of the data was accessed by the cybercriminals, and that the cybercriminals have since deleted such data. Additionally, while our cyber security consultant has found no evidence that the data was shared with others, FSOS wants to ensure that everyone is aware of the incident.

What Can Impacted Individuals Do? Although there is no evidence that employee or patient information has been misused, FSOS is making those individuals impacted aware of resources to help safeguard personal information. While FSOS has no indication that personal information has been used to commit fraud, we are here to help answer questions should they arise.