Notice of Nationwide Recovery Services, Inc. Data Security Incident

Harbin Clinic, LLC ("Harbin Clinic") is committed to protecting the confidentiality and security of its patients' information. Regrettably, Nationwide Recovery Services, Inc. ("NRS") recently notified Harbin Clinic that a data security incident experienced by NRS may have potentially involved information of Harbin Clinic patients. To date, NRS has not notified those individuals whose personal information may have been impacted. In order to best protect our patients, we are informing the public of this incident.

NRS is a third-party vendor that has provided debt collection services for delinquent accounts of individuals treated at Harbin Clinic, as well as services related to bankruptcies, lawsuits and patient estate matters. Patients or guarantors whose billing accounts were sent to collections or involved in other legal proceedings would be potentially impacted by this event.

It is our understanding that, in July 2024, NRS discovered suspicious activity related to its information technology ("IT") systems, which resulted in a network outage. NRS indicated that it determined through an investigation there was unauthorized access to the NRS network between July 5, 2024 and July 11, 2024, during which time certain files and folders were illegally copied from NRS's systems by someone without authorization. NRS reported it began a lengthy review to determine what information was contained on the impacted NRS systems and which NRS clients were impacted.

As a result of this review, NRS notified Harbin Clinic in February 2025 that information from Harbin Clinic's patients may have been present on the impacted systems, but it was not yet able to identify which individuals had been impacted. In March, NRS provided a list of individuals whose information may have been impacted by the incident. According to NRS, impacted information may have included patient name, address, Social Security number, date of birth, financial account information, guarantor information and/or medical-related information.

NRS reported that, upon becoming aware of this incident, it immediately took steps to confirm the security of its systems and to determine what information was potentially impacted, including notifying law enforcement. NRS also said it has implemented additional cybersecurity measures and reviewed existing security policies to protect against similar incidents moving forward.

While Harbin Clinic systems were not affected by this breach, Harbin Clinic has taken the following steps to address the situation and prevent future occurrences:

- Harbin Clinic immediately blocked NRS's access to Harbin Clinic systems until a forensic investigation firm determined the threat had been eradicated from the NRS network.
- Harbin Clinic conducted a review of its own systems to ensure no indicators of compromise were present in its own network.
- Harbin Clinic engaged its privacy and cybersecurity teams to conduct an investigation of the incident and work with NRS to determine the scope of the breach and identify potentially impacted Harbin Clinic patients.

Importantly, NRS reported that it has no evidence to suggest there has been identify theft or fraud related to this incident. However, as a precaution, we are notifying potentially impacted patients and their guarantors by this publication. We will also be mailing notification letters to Harbin Clinic patients and guarantors identified through NRS's review and for whom we have sufficient contact information.

Unfortunately, cyber-attacks can and do happen every day all around the world. We encourage all of our patients to routinely check their financial accounts and to consider utilizing some of the publicly available security services to help protect their identities from fraud. Federal regulatory agencies recommend remaining vigilant for 12 to 24 months following a potential exposure of personal information. The notification letter includes guidance and additional information on general steps people can take to monitor and protect their personal information.

Harbin Clinic has established a dedicated, toll-free call center at (866) 408-3081 to answer questions from those who were potentially impacted. The call center is available Monday through Friday from 9 a.m.- 6:30 p.m. Eastern Time, excluding major U.S. holidays.

We apologize for any concern or inconvenience this may have caused and remain committed to protecting the confidentiality and security of our patients' information and to working closely with our vendors to ensure they uphold our high standards for privacy protection. We have and will continue to enhance our security and vendor controls, as appropriate, to minimize the risk of similar situations in the future.

Frequently Asked Questions

1. **What happened?**

   NRS reported that, in July 2024, NRS discovered suspicious activity related to its information technology systems, which resulted in a network outage. NRS indicated that it determined through an investigation there was unauthorized access to the NRS network between July 5 and July 11, 2024, during which time certain files and folders were illegally copied from NRS's systems by someone without authorization.

2. **What personal information of mine may have been affected?**

   From NRS's investigation, it reports that potentially impacted information may have included patient name, address, Social Security number, date of birth, financial account information, guarantor information and/or medical-related information.

3. **What have you done to keep something like this from happening again?**

   We are committed to protecting the security and privacy of our patients' information. Harbin Clinic has taken the following steps to address the situation and prevent future occurrences:

   - Harbin Clinic immediately blocked NRS's access to Harbin Clinic systems until a forensic investigation firm determined the threat had been eradicated from the NRS network.

- Harbin Clinic conducted a review of its own systems to ensure no indicators of compromise were present in its own network.
- Harbin Clinic engaged its privacy and cybersecurity teams to conduct an investigation of the incident and work with NRS to determine the scope of the breach and identify potentially impacted Harbin Clinic patients.

4. Why does NRS have my information?

NRS is a third-party vendor used by Harbin Clinic to provide debt collection services for delinquent accounts of patients treated at Harbin Clinic, as well as services related to bankruptcies, lawsuits and patient estate matters. In connection with these services, Harbin Clinic shared information related to patients and their guarantors with NRS.

5. What can I do now?

It is always a good idea to review the statements you receive from your health care provider and health insurer. If you see services that you did not receive, please contact the provider or insurer immediately. As a best practice, you can also review recommendations at the Federal Trade Commission's website, www.identitytheft.gov. You can obtain information from this website about steps you can take to help avoid identity theft as well as information about fraud alerts and security freezes.