For Immediate Release

Battle Ground, WA - 06/03/2026 - We use a third party company to electronically prescribe medications and communicate directly with our patients' pharmacy. We were informed by this company that they had a data breach. This is the information that we received from them:

Networking Technology, Inc. d/b/a RXNT ("RXNT") contracts with healthcare organizations to provide cloud-based software solutions for electronic prescribing, practice management, and electronic health records. RXNT recently experienced a cybersecurity incident and is notifying individuals whose information was involved.

What Happened? On March 3, 2026, RXNT became aware of unauthorized activity on one of the RXNT solutions used by a portion of its customers. It conducted an internal investigation alongside cybersecurity experts and took steps to contain the activity and confirm that the unauthorized actor had been eliminated from the environment. RXNT also notified law enforcement. The investigation determined that, between March 1, 2026, and March 3, 2026, an unauthorized actor obtained certain data stored on the system. RXNT conducted a comprehensive review of the affected data to identify what information was involved and the individuals and customers to whom it related. RXNT notified affected customers beginning on May 1, 2026.

What Information Was Involved? The information involved varies by individual and may include patient names, dates of birth, demographic information (such as addresses, contact information and patient ID) and prescription information (such as prescribing provider, prescription, and receiving pharmacy). In limited instances, a Social Security number was also included. The incident did not involve any payment card, bank account, or other financial information.

What RXNT Is Doing. Data privacy and security are RXNT's highest priorities and RXNT takes this incident very seriously. After becoming aware of the incident, RXNT immediately took steps to contain it and, with the help of external cybersecurity experts, confirmed that the unauthorized actor was eliminated from the environment. To help prevent a similar incident from happening in the future, RXNT will continue to take steps to further strengthen the security of all of its systems and applications.

RXNT notified affected customers of this incident beginning on May 1, 2026. Since then, it has worked with customers to notify individuals whose information was involved. RXNT is also providing resources involved individuals can use to help protect their information, including complimentary credit monitoring and identity protection services for individuals whose Social Security numbers were involved in this incident.

What Individuals Can Do. While the investigation did not reveal any instances of fraud or identity theft that have occurred as a result of this incident, as a precaution, RXNT recommends individuals review relevant statements for unrecognized transactions. In the event of suspicious activity, they are encouraged to contact the associated vendor or provider immediately.

For More Information. RXNT has also established a dedicated, toll-free call center for questions about this incident. The call center may be reached at ***1 (877) 327-0287*** from 9 a.m. to 9 p.m. Eastern Time, Monday through Friday, excluding some major U.S. holidays.