VISTA
RADIOLOGY, P.C.

On July 11, 2021, Vista Radiology, P.C. (Vista) became aware that portions of its network were encrypted by an unknown malicious third-party as part of a ransomware cybersecurity attack. Vista took immediate steps to secure its patient data including immediately taking its network offline and launching an internal investigation with the assistance of a leading independent computer forensics firm. Initial findings indicated that the third-party sought to encrypt but not exfiltrate data from Vista's network. Vista was then advised on July 15, 2021 that there were indications that the attackers had accessed and viewed certain servers and folders on the Vista network containing patient data. Although only a relatively small amount of data was accessed, it could not be determined what if any specific patient information was viewed or accessed on the affected network servers and folders. Given the possibility that some patient data was compromised, Vista took steps to treat this matter as a potential breach under the Health Insurance Portability and Accountability Act (HIPAA). Vista undertook an extensive forensic investigation of its entire network to identify all areas where protected health information (PHI) may have been compromised. Additionally, Vista has reported this incident to law enforcement and continues to work with them to seek assistance in responding to the attack.

The forensic investigation to date demonstrates that certain Vista data was encrypted the evening of July 10, 2021 and that a smaller subset of that data may have been accessed during the intrusion. The investigation has not demonstrated that any significant amount of data was exfiltrated from our network. However, our investigation is ongoing and we continue to undertake additional forensic review of potentially affected data. Fortunately, Vista has been able to restore its network from back-ups and does not intend to negotiate with the malicious third-party.

To date we have no information to indicate that protected health information (PHI) was actually acquired or misused beyond the fact that it may have been stored in areas of the Vista network that were encrypted by the malicious third-party.

While the investigation does not suggest any personal data was actually acquired or misused, Vista cannot yet rule out the possibility that certain files containing patients' information may have been subject to unauthorized access. Vista has taken measures to further increase the security of our network environment, including ongoing forensic investigation and a complete rebuild and redesign of network security, to minimize the possibility of a similar event occurring in the future. Patients whose information may have been involved in this incident have been or will be sent an individual notification letter from Vista and are advised to review the statements they receive from their health care providers and health insurance plan. If individuals see services they did not receive, they should contact the provider or health plan immediately. Further, Vista is providing 12-months of no cost identity and credit monitoring to affected patients. To find out if you qualify for this offered service, please contact us through the toll-free number listed below.

We deeply regret any inconvenience or concern this incident may cause. We take this matter very seriously and are continuing to enhance our security protocols to help prevent a similar incident from occurring in the future. If you have any questions about this incident, please contact us at (855) 651-2604 Monday through Friday, between 9:00 am to 6:00 pm, Eastern Time.

Frequently Asked Questions (FAQs)

What happened?

On July 11, 2021, Vista became aware that portions of its network had been encrypted by an unknown malicious third-party as part of a ransomware cybersecurity attack. Initial investigation results demonstrate that certain Vista data was encrypted on the evening of July 10, 2021 and that a smaller subset of that data may have been accessed during the intrusion. Vista immediately took its network offline to protect the information it maintains and to secure its systems. Vista then launched a comprehensive forensic investigation with the help of a leading cybersecurity firm. Additionally, Vista has notified appropriate law enforcement agencies and continues to cooperate with them in their investigation of this incident.

When did the incident occur?

This incident occurred the evening of July 10, 2021 and was discovered by Vista IT staff later that night. Immediately upon learning of the incident, Vista took its network offline to protect its patients and secure its systems, launched an investigation, and notified law enforcement. As part of the investigation, Vista is working diligently alongside a leading independent computer forensics firm to identify what information may have been compromised. Once Vista determined what information may have been involved, it moved quickly to notify potentially affected individuals.

How do you know the systems are safe now?

Vista took its systems offline and fortified its network before bringing them back online. A comprehensive forensic investigation helped us identify and correct network vulnerabilities that may have been used by the malicious third-party. Vista's complete rebuild and hardening of its network continues but we are again operational. We believe our new network is more robust, safe, and secure.

What patient data was involved?

While an extensive forensic investigation has revealed that the malicious third-party only interacted with a small area of our network, Vista has not yet ruled out the possibility that files in that area were accessed. The area in question does contain personal health information pertaining to some Vista patients, including name, date of birth, Social Security number, radiology study performed and radiologist comments. Fortunately, the data does not contain any financial information such as banking information or credit card numbers. The investigation to date has not demonstrated that any significant amount of data was exfiltrated from the area where unauthorized access occurred. However, out of an abundance of caution, Vista is sending individual HIPAA notification letters to all affected patients where it cannot be ruled out that their information was compromised during the ransomware attack.

How is Vista responding?

Vista immediately took its network offline to protect its patient data and to secure its systems. Vista also launched an investigation and notified law enforcement. Vista continues to cooperate with law enforcement including providing technical data regarding the ransomware attack. Once Vista determined that personal information was potentially involved in this incident, it moved quickly to notify those individuals and government regulators, in accordance with applicable law. We have taken measures to further increase the security of our network environment, including ongoing forensic investigation and a complete rebuild and redesign of network security, to minimize the possibility of a similar event occurring in the future. Additionally, those patients whose information may have been affected are being offered 12-months of no cost identity and credit monitoring to help protect them if in fact their PHI has been compromised.