Notice of Virtual Private Network Solutions, LLC d/b/a VPN Solutions, LLC Data Security Incident

Louisville, Kentucky – [March 17, 2023] – Virtual Private Network Solutions, LLC d/b/a VPN Solutions, LLC ("VPN") provides electronic health record management services to health care providers. Associates in Dermatology ("AID") uses VPN's software, TouchChart, where VPN hosts AID patient information. This notice is intended to alert potentially impacted individuals of a data breach incident VPN experienced, steps we are taking in response, and resources available to assist and protect individuals.

What Happened: On or around October 31, 2021, **VPN experienced a ransomware**. VPN informed AID on December 22, 2021 that none of AID's data hosted on VPN was impacted by this incident, however a forensics investigation was still ongoing. AID followed up many times to receive a formal report of what information was impacted. On January 17, 2023, VPN informed AID that on or about November 15, 2023, they identified files pertaining to AID that potentially contained sensitive information. VPN determined that these files are tag image files from a data warehouse, **not an electronic medical record system**, the majority of which do not contain personally identifiable information and/or protected health information. VPN was able to match some files to patient names, but did not confirm if these files contained protected health information nor did VPN's list fully identify the names of individuals and the type of data that may have been compromised by the ransom attack. On March 10, 2023, AID determined that the compromised files may have also contained personally identifiable information.

AID is working to identify all the specific individuals and the type of data that was impacted by VPN's breach in order to provide sufficient notice. AID has no reason to believe that any individual's information has been misused as a result of this event.

What Information Was Involved: While we have no reason to believe that information has been misused as a result of this incident, we are notifying individuals for purposes of full transparency. The types of information that was identified by VPN as compromised varied with each individual. Based on a review of the files, the unauthorized party may have had access to: first and last name, address, social security numbers, date of birth; medical condition, medical treatment; medical diagnosis; medical test results; health insurance policy number; subscriber identification number; health plan beneficiary numbers; unique identifier used by AID to identify the individual.

What VPN Is Doing: Based on VPN's correspondence with us, VPN has represented to us the following: VPN's forensic investigation efforts to date have not been able to determine the cause or origin of the incident, including whether the incident may have been the result of access through a third-party system. Following the incident, VPN began building an entirely new environment to host its data including robust security controls and endpoint detection and response solution. VPN completed rebuilding its entire environment and restoring all data. VPN continues to maintain multiple endpoint detection and response solutions in the new environment with the use of Sentinel

One and Carbon Black EDR and is continuing to work to identify and implement measures to further strengthen the security of its systems to help prevent this from happening in the future.

What We Are Doing: AID has performed a review of its contracts with third party vendors and their cybersecurity environment. AID is also offering complimentary credit monitoring and identity theft protection services to the potentially affected individuals. Notification letters will be sent to those impacted individuals with the information to enroll in the credit monitoring services. AID strongly encourages all identified individuals to register for this free service.

What You Can Do: AID encourages all individuals to remain vigilant against incidents of identity theft and fraud, to review their account statements, and to monitor their credit reports for suspicious or unauthorized activity. Additionally, individuals should contact their financial institution and all major credit bureaus to inform them of the incident and then take whatever steps are recommended by these institutions, which may include placing of a fraud alert on the individual's account.

For More Information: For individuals seeking more information or questions about this incident, please call AID's dedicated toll-free helpline at 1-833-570-2973 between the hours of 8:00 am to 8:00 pm Central Time, Monday through Friday.

Once again, Associates in Dermatology sincerely apologizes for any inconvenience this incident may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Associates in Dermatology