Background of Netgain Incident and Frequently Asked Questions

Background of security incident

The Apple Valley Clinic provides primary care and urgent care services. The Apple Valley Clinic contracts with Netgain Technology, LLC (Netgain), to host its information technology network and computer systems.

On December 2, 2020, we were notified by Netgain that its systems had been compromised by a cyberattack. After discovering the cyberattack, Netgain notified law enforcement and ultimately regained control of its systems and recovered the affected data. On January 29, 2021 after the Netgain systems were restored, Allina Health received confirmation that the data involved in the cyberattack contained patient data. We have worked with experts to determine what patient data was affected in order to provide our patients with the most accurate information about the incident and the individuals potentially affected.

Allina Health began investigating this incident as soon as we received notice of it. In a ransomware attack, cybercriminals attempt to disrupt a business by locking companies out of their own data and servers.

What Allina Health is doing to protect personal information

We are communicating regularly with Netgain to ensure they are taking appropriate steps to better maintain the security of the Apple Valley Clinic's data. Netgain has provided written assurances that the threat to its systems has been contained and eliminated. Netgain is continuing to scan its environment to identify potential impacts from the attack and will work promptly to address any new vulnerabilities that may be identified.

We are committed to our patient's privacy and we understand that these types of events can cause concern. Although the Apple Valley Clinic was not targeted in this cyberattack, we are taking steps to enhance our own cybersecurity protocols and practices. In February, we implemented Allina Health's electronic health record system and began migrating the Apple Valley Clinic to a new information technology system, used by Allina Health.

Frequently Asked Questions:

What kind of information was involved?

This incident only impacted individuals receiving health care services at the Apple Valley Clinic. No other Allina Health locations were impacted by the incident.

The information may have included:

- Names
- Addresses
- Dates of birth
- Social Security Numbers
- Medical Information such as medical symptoms and diagnoses

- Clinical notes
- Billing information
- Credit card information
- Bank account information
- Additional medical information, such as medications and lab results

Was my information involved and how will I know?
We have sent communication to individuals whose information may have been involved.

When did the situation occur?
Allina Health was notified by our vendor in early December and immediately began an investigation. The vendor was impacted in December and conducted an investigation with law enforcement.

What measures have been take to prevent this from happening again?
We are taking steps to enhance our own cybersecurity protocols and practices. In February, we implemented Allina Health's electronic health record system and began migrating the Apple Valley Clinic to a new information technology system, used by Allina Health.

Have affected patients been notified?
Allina Health has notified those impacted by this incident. In addition, there is a link to the notice on the Apple Valley Medical Center website (applevalleymedicalcenter.com) which will be in place for the next 90 days and a press release was sent out to relevant media outlets.

How many people or patients were affected? Have those affected patients been notified? Were my children or family members also impacted?
Allina Health has notified those impacted by this incident. In addition, there is a link to the notice on the Apple Valley Medical Center website (applevalleymedicalcenter.com) which will be in place for the next 90 days and a press release was sent out to relevant media outlets.

How do you know the cybercriminal destroyed the information?
We do not know that and that is why we notified you.

I do not want my records into an electronic health record. Can you delete me from the database/system?
We need to maintain your record for continuity of care and we are required to retain your information. We do not maintain records on paper - this is not administratively possible.

Was the ransom paid?
Yes - the software vendor, Netgain, paid the ransom. This will not affect the cost of healthcare at Allina Health.

What should I do?
We are not aware that any data was disclosed or used by those responsible for the cyberattack. However, out of an abundance of caution, we are offering patients a complimentary one-year membership of Experian credit monitoring/identity protection services.

We recommend regularly reviewing the explanation of benefits provided by your health care insurer, credit card statements, and bank accounts for suspicious activity. Any unusual service or charge should be reported to the appropriate financial institution, insurer or health care program

immediately. If you suspect that someone is using your personal information to obtain medical services or incur charges without your permission, please report this to the local police department immediately. Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of the credit monitoring service offering.

I want to file a complaint; where can I do this?

You may file a complaint with the Allina Health Privacy Office by writing to the following address:

Allina Health Privacy Office
Mail Route 10811
P.O. Box 43
Minneapolis, MN 55440-0043

In addition, the federal Office for Civil Rights has been notified of this situation.

If you would like to submit an additional complaint to the Office for Civil rights you can submit your complaint on their website: (http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html), by email OCRComplaint@hhs.gov, or by mail:

Centralized Case Management Operations
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F HHH Bldg.
Washington, D.C. 20201