- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Incident Response

Additional Healthcare Firms Disclose Impact From Netgain Ransomware Attack

By Ionut Arghire on January 17, 2022

Healthcare providers Caring Communities and Entira Family Clinics are warning patients that their personal information may have been exposed in a data breach that hit tech vendor Netgain Technology more than a year ago.

In late November 2020, Netgain, which provides managed IT services to organizations in sectors such as accounting, healthcare, and legal, fell victim to a ransomware attack that also resulted in the compromise of customer data.

By January 2021, Netgain had informed affected organizations of the incident, and numerous healthcare services providers began sending data breach notices over the next several months, including Ramsey County's Family Health division, Woodcreek Provider Services, Sandhills Medical Foundation, Apple Valley Clinic, Neighborhood Healthcare, San Diego Family Care (and Health Center Partners of Southern California), SAC Health System, SouthCare Carolina, and Caravus.

During summer, more healthcare provides disclosed impact from the incident, including Minnesota Community Care, CentraCare Health and Carris Health – Willmar Lakeland Clinic, Family Health Centers of San Diego, Imperial Beach Community Clinic, and LifeLong Medical Care.

Last week, Caring Communities and Entira Family Clinics also revealed the impact from the Netgain ransomware attack and began telling patients that their personal information might have been leaked.

In addition to medical history, data that was potentially compromised in the attack includes names, addresses, and Social Security numbers, both organizations said in their notification letters.

Entira told the Maine Attorney General's Office that data of roughly 200,000 individuals was compromised in the incident. Overall, the Netgain incident appears to have impacted the data of more than 1 million patients.

Related: MRIoA Discloses Data Breach Affecting 134,000 People

Related: 400,000 Individuals Affected by Email Breach at West Virginia Health Firm

Related: Preventing a Cyber Pandemic in Healthcare

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Additional Healthcare Firms Disclose Impact From Netgain Ransomware Attack
Vulnerability in IDEMIA Biometric Readers Allows Hackers to Unlock Doors
Safari 15 Vulnerability Allows Cross-Site Tracking of Users
Critical SAP Vulnerability Allows Supply Chain Attacks
Details Published on AWS Flaws Leading to Data Leaks

Tags:

NEWS & INDUSTRY Incident Response Cybercrime