



Supporting Individuals with Disabilities for Over 30 Years

Notice of Security Incident

August 4th, 2022

Independent Case Management, Inc. (ICM) is notifying individuals whose personal information may have been involved in a recent ransomware attack where an unauthorized third party accessed and encrypted data on three servers containing historical employee and customer data. The ransomware note, dated December 24, 2021, was discovered by ICM on June 15, 2022. Upon learning of this security incident, ICM immediately engaged its third-party IT security vendor to isolate the servers and perform security scans to make sure that the network was secure and other data was not impacted.

ICM reported this incident to the FBI and began an investigation to identify which customers and employees were possibly affected. Unfortunately, ICM has not been able to determine if specific personal information was accessed or misused, but we know that data housed on the infected servers included names and addresses, dates of birth, social security numbers, health records, insurance plan and payment information, Medicaid numbers, medical and health records, and employment files of some of our customers and employees. ICM is sending letters to potentially affected individuals with details about the incident and information that can help minimize the chance that an individual's personal information could be used inappropriately. Precautions that should be taken include:

- Monitoring and reviewing health insurance claims, financial account information, and credit card statements and immediately notifying the appropriate company of any unauthorized activity.
- Registering for a free fraud alert with one of the three major credit bureaus – Equifax (www.equifax.com); Experian (www.experian.com); or TransUnion (www.transunion.com)
- Consider placing a security freeze on your credit report to restrict access and help prevent additional instances of identity theft.
- Consider filing a report with the Federal Trade Commission at: <https://www.identitytheft.gov/#/>.

ICM is committed to protecting the privacy and security of the personal information of our customers and employees. We sincerely regret that this incident occurred and have taken the following steps to help prevent recurrence:

- Performed security scans of our current systems to ensure all current electronic files are secure and have multi-factor authentication requirements for accessing certain electronic systems that house personal or health information of our customers or employees.
- Assessed additional security measures that would allow for faster detection of security threats.

- Will be providing additional cybersecurity training to all of our employees; and
- Will continue to perform periodic risk assessments and update our cybersecurity processes in response to changes in technology and as new threats arise.

If you have any questions about this security incident, please call our toll-free number at 1-800-380-9501 between 8am and 4pm.