

PERTH AMBOY:(732) 376-9333**NEWARK:**(973) 679-7709**CARTERET**(732) 376-6650

Central Jersey Medical Center Provides Notice of Data Security Incident

El Centro Médico Central Jersey Informa sobre un Incidente de Seguridad de Datos

Central Jersey Medical Center Provides Notice of Data Security Incident

Central Jersey Medical Center, Inc. ("CJMC") is issuing notice regarding a data security incident that may involve information related to certain patients of Central Jersey Medical Center. This notice provides information about the incident, the response, and resources available to individuals to help protect their information from possible misuse, should they feel it necessary to do so.

What Happened?

An external party gained access to Central Jersey Medical Center dental servers' network on August 25, 2025, and downloaded ransomware, which was used to encrypt files on our network. Upon learning of the attack, CJMC launched an investigation to secure our network and to determine the nature and scope of the activity.

What information was involved?

Our investigation has now determined that an unauthorized third-party gained access to our network and, on August 25, 2025, encrypted copies of certain data. The information involved may include demographic information (such as name, date of birth, address, telephone number, email address, race or ethnicity), Social Security number, dental record number, health insurance information, dental diagnoses, treatment history, and/or billing information.

Central Jersey Medical Center's electronic medical record system was not involved nor accessed in this incident, and no financial accounts or payment information was included.

While we have no evidence that patient information has been misused, we are notifying patients out of an abundance of caution so you can take steps to protect yourself.

How will I know if my data was impacted?

We take the security of our patients' information very seriously. At this time, there is no evidence that patient information has been misused

What is Central Jersey Medical Center doing?

Upon discovering this incident, we took immediate steps to secure our systems and prevent any further unauthorized access. Our ongoing response includes:

- Engaging external cybersecurity experts to assist with our investigation and to enhance our security measures.
- Reviewing our internal procedures and strengthening our technical safeguards to prevent a recurrence.
- Additional safeguards are being implemented to prevent similar incidents in the future.
- We notified law enforcement authorities and are cooperating with their investigation.
- Reporting this matter to the federal and state authorities and agencies as required

We are committed to fully complying with all state and federal requirements and maintaining timely and transparent communication with our patients and the community. Also, we are committed to protecting your information and sincerely apologize for any concern or inconvenience this incident may cause you.

What you can do?

While we are not aware of any misuse of patient information at this time, as a precautionary measure, we recommend that you remain vigilant and take the following steps to protect your information:

- Monitor your credit reports. You are entitled to a free credit report from each of the major credit reporting agencies once every 12 months. You can visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.
- Place a Fraud Alert: Consider placing a fraud alert on your credit file with the three major credit bureaus. A fraud alert advises businesses to take extra steps to verify your identity before opening new credit.
 - o Equifax: 1-800-685-1111 | www.equifax.com
 - o Experian: 1-888-397-3742 | www.experian.com
 - o TransUnion: 1-800-916-8800 | www.transunion.com
- Monitor Your Accounts: Check your bank and credit card statements for any fraudulent activity.
- Review your account statements. Carefully check your dental and health insurance explanation of benefits (EOB) statements for any unfamiliar services or activity.
- For Social Security Numbers involved: You can place a credit freeze on your files with the three major credit bureaus. This prevents new credit from being opened in your name.

For More Information

We deeply regret this incident and any concern it may cause. If you have any questions or require further information, please call us at our dedicated

telephone number: (732) 376-6697, Monday through Friday, 9:00 AM to 5:00 PM,
EST, except holidays

Sincerely,

John O'Leary
Chief Executive Officer
Central Jersey Medical Center

El Centro Médico Central Jersey Informa sobre un Incidente de Seguridad de Datos

Central Jersey Medical Center, Inc. ("CJMC") emite este aviso con respecto a un incidente de seguridad de datos que puede involucrar información relacionada con ciertos pacientes del Centro Médico Central Jersey. Este aviso proporciona información sobre el incidente, la respuesta y los recursos disponibles para ayudar a las personas a proteger su información de un posible uso indebido, en caso de que consideren necesario hacerlo.

¿Qué ocurrió?

El 25 de agosto de 2025, una parte externa obtuvo acceso a la red de servidores dentales del Centro Médico Central Jersey y descargó un programa de ransomware, el cual fue utilizado para encriptar archivos en nuestra red. Al enterarnos del ataque, CJMC inició una investigación para asegurar nuestra red y determinar la naturaleza y el alcance de la actividad.

¿Qué información se vio comprometida?

Nuestra investigación determinó que un tercero no autorizado accedió a nuestra red y, el 25 de agosto de 2025, encriptó copias de ciertos datos. La información involucrada puede incluir datos demográficos (como nombre, fecha de nacimiento, dirección, número de teléfono, dirección de correo electrónico, raza o etnicidad), número de Seguro Social, número de historial dental, información del seguro de salud, diagnósticos dentales, historial de tratamiento y/o información de facturación.

El sistema de registros médicos electrónicos del Centro Médico Central Jersey no estuvo involucrado ni fue accedido en este incidente, y no se incluyó información financiera ni de pagos.

Aunque no tenemos evidencia de que la información de los pacientes haya sido utilizada de manera indebida, estamos notificando a los pacientes por precaución, para que puedan tomar medidas de protección si así lo desean.

¿Cómo sabré si mis datos se vieron afectados?

Nos tomamos muy en serio la seguridad de la información de nuestros pacientes. En este momento, no hay evidencia de que la información de los pacientes haya sido utilizada indebidamente.

¿Qué está haciendo el Centro Médico Central Jersey?

Al descubrir este incidente, tomamos medidas inmediatas para asegurar nuestros sistemas y prevenir cualquier acceso no autorizado adicional. Nuestra respuesta en curso incluye:

- Contratar expertos externos en ciberseguridad para que nos asistan con la investigación y fortalezcan nuestras medidas de seguridad.
- Revisar nuestros procedimientos internos y reforzar nuestras protecciones técnicas para evitar que vuelva a ocurrir.
- Implementar salvaguardas adicionales para prevenir incidentes similares en el futuro.

- Notificar a las autoridades policiales y cooperar con su investigación.
- Reportar este asunto a las autoridades y agencias federales y estatales según lo requerido.

Estamos comprometidos a cumplir plenamente con todos los requisitos estatales y federales, y a mantener una comunicación transparente y oportuna con nuestros pacientes y la comunidad. Así mismo, reafirmamos nuestro compromiso con la protección de su información y ofrecemos nuestras más sinceras disculpas por cualquier preocupación o inconveniente que este incidente pueda ocasionar.

¿Qué puede hacer usted?

Aunque no estamos al tanto de un uso indebido de la información de los pacientes en este momento, como medida de precaución, recomendamos que se mantenga vigilante y tome los siguientes pasos para proteger su información:

- Monitoree sus informes de crédito. Tiene derecho a obtener un informe de crédito gratuito de cada una de las agencias de crédito principales una vez cada 12 meses. Puede visitar www.annualcreditreport.com o llamar gratuitamente al 1-877-322-8228.
- Coloque una alerta de fraude. Considere colocar una alerta de fraude en su archivo de crédito con las tres agencias de crédito principales. Una alerta de fraude advierte a las empresas que deben tomar medidas adicionales para verificar su identidad antes de abrir un nuevo crédito.
 - Equifax: 1-800-685-1111 | www.equifax.com
 - Experian: 1-888-397-3742 | www.experian.com
 - TransUnion: 1-800-916-8800 | www.transunion.com
- Monitoree sus cuentas. Revise sus estados de cuenta bancarios y de tarjetas de crédito para detectar cualquier actividad fraudulenta.
- Revise sus estados de beneficios. Verifique cuidadosamente las explicaciones de beneficios (EOB) de su seguro dental y médico para asegurarse de que no haya servicios o actividades desconocidas.

· Para los números de Seguro Social involucrados: Puede colocar un congelamiento de crédito en sus archivos con las tres agencias de crédito principales. Esto evita que se abra nuevo crédito a su nombre.

Para más información

Lamentamos profundamente este incidente y cualquier preocupación que pueda causar. Si tiene preguntas o necesita más información, por favor llámenos a nuestro número telefónico dedicado: (732) 376-6697, de lunes a viernes, de 9:00 AM a 5:00 PM (hora del Este), excepto días festivos.

Atentamente,

John O'Leary
Director Ejecutivo
Central Jersey Medical Center

Quick Links