

Notice of Data Event

Mediko was recently notified that CorrectCare Integrated Health (CorrectCare), an outside vendor Mediko uses for medical claims processing, experienced an incident that may impact the security of certain patient data stored by CorrectCare. CorrectCare will be sending notice letters directly to those who are impacted, for whom they have a current mailing address. Mediko is also providing this notice to those who may not be receiving a letter from CorrectCare but who may be affected by the incident, and to those who would like more information about the incident. Mediko is also notifying appropriate state and federal regulators.

What Happened?

On July 6, 2022, CorrectCare, a third-party health administrator used by Mediko to process medical claims information for our patients, discovered that two file directories on CorrectCare's web server had been inadvertently exposed to the public internet. The file directories contained protected health information (PHI) of certain individuals who were incarcerated in a Mediko facility. Upon discovery of the data exposure, CorrectCare took immediate steps to remediate the exposure by securing the server in less than nine (9) hours. Subsequently, CorrectCare engaged a third-party cybersecurity firm to conduct a forensic investigation to analyze the nature and scope of the incident. The investigation determined that patients who received medical care through Mediko between January 1, 2012, and July 7, 2022, were among those whose data was potentially impacted. CorrectCare's investigation revealed that a misconfigured web server led to exposure of patient information contained in these file directories as early as January 22, 2022.

What information was involved?

The patient information contained in the file directories included full name, date of birth, inmate number, and limited health information, such as a diagnosis code and/or CPT code, treatment provider name, and dates of treatment, and may have included a Social Security number. **Please note that the patient information stored in these file directories did not include driver's license numbers, financial account information, or debit or credit card information.** While CorrectCare has no reason to believe that any patient's information has been misused, they are nonetheless notifying all affected patients out of an abundance of caution.

What We Are Doing?

CorrectCare takes the protection of personal information seriously, and they have taken and will continue to take steps to prevent a similar occurrence. Upon discovery of this incident, CorrectCare, with assistance of leading cybersecurity specialists, has implemented specific steps to further enhance the security of its systems and further protect the information of its clients and those under its care.

Why did CorrectCare have access to my information to begin with?

CorrectCare has a Business Associate Agreement (BAA) with and helps manage health care claims on behalf of Mediko, a HIPAA covered entity, and therefore had authorized access to this personal health information.

Does this mean I'm a victim of identity theft?

No. At this point in time, CorrectCare does not have any evidence to believe that any of the information involved in this incident has been used to commit fraud. CorrectCare wanted to inform those that may have been impacted so that they can take the appropriate steps to protect themselves.

If I'm an incarcerated person, and my information was accessed, what should I do?

If you are an incarcerated individual and your information was involved in this incident, keep a copy of this notice for your records in case of future problems with your medical or financial records. You are encouraged to take advantage of the **complimentary** 12-month membership of Experian's IdentityWorks that CorrectCare is offering. To enroll in this service, please follow the instructions in the "**Steps You Can Take to Help Protect Your Personal Information**" below by February 28, 2023. This product provides you with superior identity detection and resolution of identity theft.

[Please note: your Correctional Counselor and other institutional staff do not have information on this issue. We strongly encourage you to use the resources below.]

If I am no longer an incarcerated person and my information was accessed, what should I do?

If you are no longer an incarcerated individual, but were previously incarcerated and received medical care at one of the CDCR prisons between January 2012 and July 2022, you should keep a copy of this notice for your records in case of future problems with your medical or financial records. We encourage you to review the "**Steps You Can Take to Help Protect Your Personal Information**" below by February 28, 2022.

What You Can Do

Although CorrectCare is not aware of any instances of misuse of any patient information, all individuals impacted by this incident are advised to monitor their personal information and accounts. We also encourage you to remain vigilant and review the Steps You Can Take To Help Protect Your Personal Information.

For More Information

We sincerely regret any inconvenience or concern that this Incident may cause you, and we remain dedicated to ensuring the privacy and security of all information in our control. If you have further questions or concerns, please call CorrectCare's dedicated assistance line toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays), **(844) 700-1314**. Please be prepared to provide your engagement number **B079693**.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

To help protect your identity, CorrectCare is offering a complimentary 12-month membership of Experian's IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** February 28, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: experianidworks.com/plus
- Provide your **activation code**: YJWF423PWC

Be prepared to provide engagement number **B079693** as proof of eligibility for the Identity Restoration services by Experian. If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(844) 700-1314** by February 28, 2023.

ADDITIONAL DETAILS REGARDING YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Dark Web Monitoring**
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (insert phone number). If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on

a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.