

# Data Breach at CorrectCare

Integrated Health (CCIH), a third-party administrator under contract with the Health Net Federal Services (HNFS), Business Associate of California Correctional Health Care Services and California Department of Corrections and Rehabilitation (CCHCS/CDCR), discovered that two file directories on CorrectCare's webserver had been inadvertently exposed to the public internet. The file directories contained patients' health information protected under the Health Insurance Portability and Accountability Act (HIPAA).

## What Happened?

On July 6, 2022, CorrectCare confirmed that a breach of regulated information occurred when a misconfigured web server led to exposure of patient information contained in two file directories as early as January 22, 2022. CorrectCare's security processes were able to detect and remediate the exposure in less than nine hours after discovery. Correct Care immediately engaged a third-party cybersecurity firm to conduct a forensic investigation to analyze the nature and scope of the incident. Between September 1, 2022, and October 5, 2022, the investigation determined that at least 438,000 CDCR inmates/

patients who received medical care between January 1, 2012 and July 6, 2022 were among those individuals whose data was potentially impacted. CorrectCare cannot confirm that any patients' personal information was copied from its web site or used inappropriately. However, it is notifying the public because protected health information was accessible to unauthorized persons.

## What Information was involved?

The patient information involved in the data exposure included full name, dates of birth, social security number, and limited health information, such as diagnosis code and/or Current Procedure Terminology (CPT) code.

## What is CorrectCare Doing?

Correct Care takes the privacy and confidentiality of patient information seriously. CorrectCare has hired cybersecurity experts to conduct forensic investigation and have implemented specific steps to further enhance the security of its systems and further protect the information of its clients. CorrectCare also conducted multiple searches to confirm the exposed data were not available on the dark web and contacted the federal and state regulatory agencies. The security and confidentiality

of patients' health information is critical to CorrectCare. While there is no indication that any protected health information was used inappropriately, CorrectCare is notifying affected individuals that their information was potentially compromised. CorrectCare is also offering complimentary 12-month membership of Experian's IdentityWorks to access credit and identity theft monitoring services, including dark web monitoring for one year to any individuals impacted by this event.

Any individual who believes their data may have been exposed are encouraged to enroll in Experian's IdentityWorksSM by visiting [experianidworks.com/plus](https://experianidworks.com/plus) (use Activation Code YJWF423PWC) or calling toll-free 844-700-1314 (reference Engagement Number B079693 and Activation Code YJWF423PWC) for additional information, Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Any questions regarding this matter also can be sent to: CorrectCare Privacy Office, PO Box 1178, Montebello, CA 90640.

THIS IS A PAID ADVERTISEMENT