

**Subject:** Notice of Data Breach

**From:**

**Date:** Thu, Apr 24, 2025 at 12:19 PM

**Subject:** Notice of Data Breach

**To:**

[View this email in your browser](#)



April 24, 2025

### Notice of Data Breach

Dear Valued Client,

Northern California Children's Therapy Center ("NCCTC") values and respects the privacy of your and your child's information, which is why NCCTC is writing to advise you of an incident that may have involved certain information related to your participation in the Help Me Grow Yolo County Program (the "HMGYC Program"). **While NCCTC has no reason to believe that your information has been misused for the purpose of committing fraud or identity theft**, NCCTC is issuing this notice out of an abundance of caution and in alignment with its commitment to privacy, transparency and regulatory requirements.

#### ***What Happened:***

NCCTC provides developmental screenings through the HMGYC Program, funded by First 5 Yolo through an agreement with Yolo County (the "Funding Agencies"). Like community programs providing early childhood services, NCCTC relies on a cloud-based file system to collect and manage information in order to facilitate developmental screenings and connect families with appropriate resources. This system houses the screening records.

On March 16, 2025, an unauthorized third party identified a vulnerability in the system and was able to access a limited number of records. Upon discovery of the issue, NCCTC acted immediately to secure the system and prevent further exposure. By March 19, 2025, NCCTC resolved the technical issue and fully secured the platform.

NCCTC has since completed a thorough internal review and is working closely with IT and cybersecurity experts to investigate the situation and ensure the ongoing security of its systems and patient records.

#### ***What Information Was Involved:***

The information that may have been impacted includes data entered into the screening records, including the following:

- Information about the referring provider such as the agency's name, address, phone number and the provider's name and email address;
- Information about the child such as their name, gender, date of birth and home language(s), and their developmental skills;
- Information about the parent/caregiver such as their name, relationship to the child, preferred method of contact, phone number and email address; and their broad health-related issues; and
- Broad questions or concerns of the family or provider.

While NCCTC is uncertain whether your or your child's personal information was accessed, as a precautionary measure, NCCTC is notifying you of this potential exposure. There was **no disclosure** of other types of personal information such as your Social Security number, driver's license, bank or credit card information, or health insurance information.

***What NCCTC is Doing:***

NCCTC takes the security of you and your child's information very seriously, and NCCTC is committed to maintaining your privacy. As soon as the issue was identified, NCCTC took immediate action to protect the information involved. NCCTC promptly secured and reconfigured the impacted storage system, notified the Funding Agencies and began a collaborative review. A full internal investigation was initiated to assess the scope of the incident and NCCTC engaged with cybersecurity and compliance experts to further strengthen its data protection measures. NCCTC has also continued to monitor the system for any irregular activity or concerns related to the program.

***What You Can Do:***

While NCCTC cannot confirm whether your personal information was misused, it is possible that it was accessed as part of this incident. NCCTC encourages you to remain vigilant and monitor your accounts for any unusual or suspicious activity. For your protection, NCCTC has included a sheet with additional guidance on steps you can take to help safeguard your personal information.

***For More Information:***

Should you have questions regarding this matter, please do not hesitate to contact NCCTC by calling (888) 588-4174, Monday through Friday, between the hours of 9am to 5pm Pacific Standard Time for assistance.

Respectfully,

Northern California Children's Therapy Center  
1321 College Street, Suite E  
Woodland, CA 95698

**Steps You Can Take to Protect Your Information**

***Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:***

As a precautionary measure, NCCTC recommends that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. Additionally, you should report any fraudulent activity or suspected incidence of identity theft to proper law enforcement authorities, including local law enforcement to file a police report, the Attorney General, or the FTC. To file a complaint with the FTC, go to [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. A copy of Take Charge: Fighting Back Against Identity Theft, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the following website: <https://www.ojp.gov/ncjrs/virtual-library/abstracts/take-charge-fighting-back-against-identity-theft>

***Copy of Credit Report:***

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com> or calling 877-322-8228; or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies is provided below.

***Fraud Alert:***

You may also consider placing a fraud alert on your credit report. An initial fraud alert is free and will remain on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the information below: