P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/cps-matter

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>> or <<IMB>>

February XX, 2025

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

CPS Solutions, LLC ("CPS Solutions"), which helps support pharmacy operations, is writing to inform you of a recent cybersecurity incident that may have affected your personal information. CPS Solutions works with certain hospitals and health care providers to help patients receive medications at a reduced cost or for free, including not limited to [HOSPITAL NAME], from which you may have received services.

What Happened:
On December 4, 2024, CPS Solutions discovered that an unauthorized third party gained access to one CPS Solutions employee's O365 business email account. Upon discovery, CPS Solutions immediately forced a password reset, disabled the email account, and took other appropriate steps to prevent further access. The email account was secured that same day and an investigation was launched to determine the potential scope and impact. Our findings indicate that an unauthorized third-party was able to access and remove data from the account, which may have contained limited personal information, between December 2 to 4, 2024. We notified your health care provider of this incident on February 10, 2025.

What Information was Involved:
The personal information involved may have included: (1) full name, date of birth, and address; (2) health insurance information (such as member/group ID number or Medicaid/Medicare number); and/or (3) medical information (such as medical record number or patient account number, clinical information, provider information, diagnosis or treatment information, or prescription information such as medication name). Not all data elements were involved for every potentially affected individual.

For the majority of potentially affected individuals, Social Security numbers were not impacted. Driver's license numbers, credit and debit card information, bank account information, test results, images, and hospital medical records were also not involved in this incident.

What We Are Doing:
CPS Solutions takes privacy and security seriously. As soon as the incident was discovered, we took immediate action to mitigate and remediate the incident and to help prevent further unauthorized activity. In response to this incident, security and monitoring capabilities are being enhanced and systems are being hardened as appropriate to minimize the risk of similar incidents in the future.

What You Can Do:
We are not aware of any misuse of individuals' information as a result of this incident to date. As a precaution to help you detect any possible misuse of your personal information, we are offering you two (2) years of free credit monitoring

and identity protection services through IDX. Details of your complimentary membership are enclosed in the Reference Guide along with instructions for registering for this service. The enclosed Reference Guide provides additional steps you may take to help monitor and protect your personal information. We also encourage you to carefully review statements sent from healthcare providers and insurance companies to ensure that all of your account activity is valid. Any questionable charges should be promptly reported to the provider or company with which you maintain the account.

For More Information:
If you have any questions regarding this notice or would like additional information, please contact us toll-free at 1-877-332-4437 between 8:00 AM to 8:00 PM CT, Monday through Friday, except holidays.

We deeply regret any concern this incident may cause you and want to assure you that we take this matter seriously.

Sincerely,

Privacy Officer
CPS Solutions, LLC

Enclosures

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

How to Enroll in IDX Credit Monitoring Services

You may enroll, at no cost to you, in online credit monitoring and identity restoration services provided by IDX for two years. To enroll in these services, please call IDX at 1-877-332-4437 or visit https://response.idx.us/cps-matter. Please note the deadline to enroll is May 10, 2025.

Individuals must enroll in order for the available services to go into effect, and the monitoring included in the membership must be activated to be effective. Please note that credit monitoring services may not be available for individuals who have not established credit or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. If you need assistance, IDX will be able to assist you.

We encourage you to take advantage of these protections and remain vigilant for incidents of potential fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the following contact information: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft/.

For Residents Of	Additional Information
District of Columbia	You may contact the D.C. Attorney General's Office to obtain information about steps to take to avoid identity theft: D.C. Attorney General's Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, www.oag.dc.gov.
Iowa	You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at: Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov.
Maryland	You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, http://www.marylandattorneygeneral.gov/.
Massachusetts	You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New Mexico	New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number, password or similar device provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report. A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone. A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act. If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.
New York	You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.
North Carolina	You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov.
Oregon	State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.
Rhode Island	You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Office of the Attorney General, 150 South Main Street, Providence, RI, 02903, 1-401-274-4400, www.riag.ri.gov.