ATTACHMENT A:
WASHINGTON – DATA BREACH NOTIFICATION

We are writing on behalf of CPS Solutions, LLC ("CPS Solutions" or "the company") to notify you of a data security incident. CPS Solutions helps support pharmacy operations of hospital and health care provider customers. At this time, CPS Solutions is providing this notice on behalf of WhidbeyHealth, a health care provider customer, with respect to 551 potentially affected Washington residents.

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, the company immediately forced a password reset, disabled the email account, and took other appropriate steps to prevent further unauthorized access. The email account was secured that same day and an investigation was launched to determine the potential scope and impact. The company's 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. This account is separate from CPS Solutions' internal network and systems, which were not affected by this incident. To date, the company is not aware of any misuse of the data.

CPS Solutions takes privacy and security seriously. As soon as the incident was discovered, the company 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 similar incidents in the future.

On January 24, 2025, CPS Solutions completed a comprehensive review which identified all customers and individuals potentially affected by this incident and what information was involved. Not all CPS Solutions customers were affected. CPS Solutions will be mailing notice letters to potentially affected individuals on behalf of affected health care provider customers who delegate the notification process to CPS Solutions. At the conclusion of the individual notice mailings, CPS Solutions will be amending this placeholder report as appropriate.

The personal information involved for the 551 potentially affected Washington residents may have included: full name, date of birth, clinical information, provider location, and medical record number or patient account number. Please note that not all data elements were involved for all individuals. ***Social Security number, driver's license number, credit and debit card information, bank account information, health insurance information, test results, images, hospital medical records and account passwords were NOT involved for these residents.***

A copy of the notifications being sent to these residents on February 10, 2025 by first class mail in accordance with notification requirements under the federal Health Insurance Portability and Accountability Act is attached to this form. CPS Solutions is also offering potentially affected individuals two (2) years of free credit monitoring and identity protection services through IDX.

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

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

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

February 11, 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. You may have received services from one of these hospitals and/or providers.

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 December 12, 2024.

What Information was Involved:
Based on our review, the personal information involved may have included: full name, date of birth, clinical information, provider location, and medical record number or patient account number. For a small subset of individuals, some prescription information (such as medication name) may have been involved. Please note that not all data elements were involved for all individuals. ***Your Social Security number, driver's license number, credit and debit card information, bank account information, health insurance information, test results, images, hospital medical records and account passwords were 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 11, 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
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.
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.

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

To the Parent or Legal Guardian of:
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>> or <<IMB>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

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

February 11, 2025

Notice of Data Breach

Dear Parent or Legal Guardian of <<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 child's personal information. CPS Solutions works with certain hospitals and health care providers to help patients receive medications at a reduced cost or for free. Your child may have received services from one of these hospitals and/or providers.

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 December 12, 2024.

What Information was Involved:
Based on our review, the personal information involved may have included: full name, date of birth, clinical information, provider location, and medical record number or patient account number. For a small subset of individuals, some prescription information (such as medication name) may have been involved. Please note that not all data elements were involved for all individuals. ***Your child's Social Security number, driver's license number, credit and debit card information, bank account information, health insurance information, test results, images, hospital medical records and account passwords were 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 child's personal information, we are offering your child two (2) years of free

identity protection services through IDX. Details of your child's 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 child's personal information. We also encourage you to carefully review statements sent from healthcare providers and insurance companies to ensure that all account activity is valid. Any questionable charges should be promptly reported to the provider or company with which the account is maintained.

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 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 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 Identity Monitoring Services

You may enroll your child, at no cost to you, in online 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 11, 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. Enrolling in this service will not affect your child's 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/.

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

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

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

February 11, 2025

Notice of Data Breach

To the Estate of <<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 the decedent's personal information. CPS Solutions works with certain hospitals and health care providers to help patients receive medications at a reduced cost or for free. The decedent may have received services from one of these hospitals and/or providers.

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 December 12, 2024.

What Information was Involved:
Based on our review, the personal information involved may have included: full name, date of birth, clinical information, provider location, and patient account number. For a small subset of individuals, some prescription information (such as medication name) may have been involved. Please note that not all data elements were involved for all individuals. ***The decedent's Social Security number, driver's license number, credit and debit card information, bank account information, health insurance information, test results, images, hospital medical records and account passwords were 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 the decedent's personal information, we are offering the decedent two (2) years of free

credit monitoring and identity protection services through IDX. Details of the decedent's 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 the decedent's personal information. We also encourage you to carefully review statements sent from healthcare providers and insurance companies to ensure that all account activity is valid. Any questionable charges should be promptly reported to the provider or company with which the account is maintained.

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 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 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 the decedent, 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 11, 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. 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/.