GenRx™

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>,

GenRx Pharmacy ("GenRx") values our relationship with our patients and respects the security of your information. We are writing to notify you about a data security incident we recently experienced and the steps we have taken in response. Although we are not aware of any actual harm to anyone as a result of this security incident, the cyberattack against GenRx did involve your personal information. Please note, neither your social security number nor any of your financial information was involved. We recognize the concern this may cause, and we deeply regret that this incident occurred.

WHAT HAPPENED?
On September 28, 2020, GenRx found evidence of ransomware on our system and immediately began an investigation, including hiring independent information security and technology experts to assist with incident response and forensic investigation. In a ransomware attack, cybercriminals attempt to disrupt the business by locking the business out of its own data. During the ransomware attack against GenRx, we had full access to all data with unaffected backups, and we were able to maintain continuous business operations as we investigated.

Together with forensic experts, GenRx terminated the cybercriminal's access to GenRx systems the same day (September 28, 2020) and confirmed that an unauthorized third party deployed the ransomware only one day before (September 27, 2020). On November 11, 2020, we confirmed that the cybercriminal was able to remove a small number of files that included certain health information GenRx used to process and ship prescriptions.

WHAT INFORMATION WAS INVOLVED?
The cybercriminals accessed and removed the following health information about you: patient ID, transaction ID (a number generated to process the prescription, not related to your financials), first and last name, address, phone number, date of birth, gender, allergies, medication list, health plan information (including member ID), and prescription information. **Please be assured that your social security number and your financial information were <u>not</u> affected. We do not collect your SSN or maintain financial information, so there is no way that cybercriminals could access this information on GenRx systems.**

WHAT WE ARE DOING.
After becoming aware of this incident, we took prompt action to secure our system to help ensure that the cybercriminal no longer had access. The cybercriminal had access to our systems for only a few hours. In addition to our existing security measures, GenRx has upgraded firewall firmware, added additional anti-virus and web-filtering software, instituted multifactor authentication, increased Wi-Fi network-traffic monitoring, provided additional training to employees, updated internal policies and procedures, and installed real-time intrusion detection and response software on all workstations and servers that access the company network. GenRx is also assessing further options to enhance our protocols and controls, technology, and training, including strengthening encryption.

WHAT YOU CAN DO.
While neither your social security number nor your financial information was affected, we wanted to provide you with some best practice recommendations. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your financial institutions or company with which the account is maintained, as well as applicable authorities, including your state attorney general and the Federal Trade Commission. Please see the Attachment for additional resources.

FOR MORE INFORMATION.
For further information and assistance, please contact 877-835-1827 between 9am – 9pm Eastern Time, Monday through Friday.

Sincerely,

Richelle Aldrich
Executive Vice President, Architecture, Business Analytics & Operations
GenRx Pharmacy

ATTACHMENT FOR COLORADO, ILLINOIS, AND WASHINGTON, DC RESIDENTS
ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
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 *www.annualcreditreport.com*, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

You may also decide 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 for the purpose of requesting a copy of your credit report or for general information is listed here:

Equifax
1-800-685-1111
www.equifax.com/CreditReport Assistance
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com/fraud
P.O. Box 1000
Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze free of charge on your credit files and fraud alerts. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay 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 contact information listed above.

FOR WASHINGTON D.C. RESIDENTS
You can obtain information about preventing identify theft from the FTC or the following:
Washington D.C. Attorney General:
Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

GenRx™

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>,

GenRx Pharmacy ("GenRx") values our relationship with our patients and respects the security of your information. We are writing to notify you about a data security incident we recently experienced and the steps we have taken in response. Although we are not aware of any actual harm to anyone as a result of this security incident, the cyberattack against GenRx did involve your personal information. Please note, neither your social security number nor any of your financial information was involved. We recognize the concern this may cause, and we deeply regret that this incident occurred.

WHAT HAPPENED?
On September 28, 2020, GenRx found evidence of ransomware on our system and immediately began an investigation, including hiring independent information security and technology experts to assist with incident response and forensic investigation. In a ransomware attack, cybercriminals attempt to disrupt the business by locking the business out of its own data. During the ransomware attack against GenRx, we had full access to all data with unaffected backups, and we were able to maintain continuous business operations as we investigated.

Together with forensic experts, GenRx terminated the cybercriminal's access to GenRx systems the same day (September 28, 2020) and confirmed that an unauthorized third party deployed the ransomware only one day before (September 27, 2020). On November 11, 2020, we confirmed that the cybercriminal was able to remove a small number of files that included certain health information GenRx used to process and ship prescriptions.

WHAT INFORMATION WAS INVOLVED?
The cybercriminals accessed and removed the following health information about you: patient ID, transaction ID (a number generated to process the prescription, not related to your financials), first and last name, date of birth, gender, medication list, health plan information (including member ID), and prescription information. **Please be assured that your social security number and your financial information were <u>not</u> affected. We do not collect your SSN or maintain financial information, so there is no way that cybercriminals could access this information on GenRx systems.**

WHAT WE ARE DOING.
After becoming aware of this incident, we took prompt action to secure our system to help ensure that the cybercriminal no longer had access. The cybercriminal had access to our systems for only a few hours. In addition to our existing security measures, GenRx has upgraded firewall firmware, added additional anti-virus and web-filtering software, instituted multifactor authentication, increased Wi-Fi network-traffic monitoring, provided additional training to employees, updated internal policies and procedures, and installed real-time intrusion detection and response software on all workstations and servers that access the company network. GenRx is also assessing further options to enhance our protocols and controls, technology, and training, including strengthening encryption.

WHAT YOU CAN DO.
While neither your social security number nor your financial information was affected, we wanted to provide you with some best practice recommendations. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your financial institutions or company with which the account is maintained, as well as applicable authorities, including your state attorney general and the Federal Trade Commission. Please see the Attachment for additional resources.

FOR MORE INFORMATION.
For further information and assistance, please contact 877-835-1827 between 9am - 9pm Eastern Time, Monday through Friday.

Sincerely,

Richelle Aldrich
Executive Vice President, Architecture, Business Analytics & Operations
GenRx Pharmacy

ATTACHMENT FOR COLORADO, ILLINOIS, AND WASHINGTON, DC RESIDENTS
ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
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 *www.annualcreditreport.com*, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

You may also decide 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 for the purpose of requesting a copy of your credit report or for general information is listed here:

Equifax
1-800-685-1111
www.equifax.com/CreditReport Assistance
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com/fraud
P.O. Box 1000
Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze free of charge on your credit files and fraud alerts. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay 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 contact information listed above.

FOR WASHINGTON D.C. RESIDENTS
You can obtain information about preventing identify theft from the FTC or the following:
Washington D.C. Attorney General:
Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
TO THE PARENT OR GUARDIAN OF:
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear Parent or Guardian of <<Name 1>>,

GenRx Pharmacy ("GenRx") is writing to you as the parent or guardian of a minor GenRx patient. GenRx values our relationship with our patients and respects the security of your minor's information. We are writing to notify you about a data security incident we recently experienced and the steps we have taken in response. Although we are not aware of any actual harm to anyone as a result of this security incident, the cyberattack against GenRx did involve your minor's personal information. Please note, neither your minor's social security number nor any of your minor's financial information was involved. We recognize the concern this may cause, and we deeply regret that this incident occurred.

WHAT HAPPENED?
On September 28, 2020, GenRx found evidence of ransomware on our system and immediately began an investigation, including hiring independent information security and technology experts to assist with incident response and forensic investigation. In a ransomware attack, cybercriminals attempt to disrupt the business by locking the business out of its own data. During the ransomware attack against GenRx, we had full access to all data with unaffected backups, and we were able to maintain continuous business operations as we investigated.

Together with forensic experts, GenRx terminated the cybercriminal's access to GenRx systems the same day (September 28, 2020) and confirmed that an unauthorized third party deployed the ransomware only one day before (September 27, 2020). On November 11, 2020, we confirmed that the cybercriminal was able to remove a small number of files that included certain health information GenRx used to process and ship prescriptions.

WHAT INFORMATION WAS INVOLVED?
The cybercriminals accessed and removed the following health information about your minor: patient ID, transaction ID (a number generated to process the prescription, not related to your or your minor's financials), first and last name, address, phone number, date of birth, gender, allergies, medication list, health plan information (including member ID), and prescription information. **Please be assured that your minor's social security number and your minor's financial information were <u>not</u> affected. We do not collect your minor's SSN or maintain financial information, so there is no way that cybercriminals could access this information on GenRx systems.**

WHAT WE ARE DOING.
After becoming aware of this incident, we took prompt action to secure our system to help ensure that the cybercriminal no longer had access. The cybercriminal had access to our systems for only a few hours. In addition to our existing security measures, GenRx has upgraded firewall firmware, added additional anti-virus and web-filtering software, instituted multifactor authentication, increased Wi-Fi network traffic monitoring, provided additional training to employees, updated internal policies and procedures, and installed real-time intrusion detection and response software on all workstations and servers that access the company network. GenRx is also assessing further options to enhance our protocols and controls, technology, and training, including strengthening encryption.

WHAT YOU CAN DO.
While neither your minor's social security number nor your minor's financial information was affected, we wanted to provide you with some best practice recommendations. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your minor's account statements and monitoring free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to the financial institutions or company with which the account is maintained, as well as applicable authorities, including your state attorney general and the Federal Trade Commission. Please see the Attachment for additional resources.

FOR MORE INFORMATION.
For further information and assistance, please contact 877-835-1827 between 9am - 9pm Eastern Time, Monday through Friday.

Sincerely,

Richelle Aldrich
Executive Vice President, Architecture, Business Analytics & Operations
GenRx Pharmacy

ATTACHMENT FOR COLORADO, ILLINOIS, AND WASHINGTON, DC RESIDENTS
ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
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 *www.annualcreditreport.com*, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

You may also decide 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 for the purpose of requesting a copy of your credit report or for general information is listed here:

Equifax
1-800-685-1111
www.equifax.com/CreditReport Assistance
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com/fraud
P.O. Box 1000
Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze free of charge on your credit files and fraud alerts. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay 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 contact information listed above.

FOR WASHINGTON D.C. RESIDENTS
You can obtain information about preventing identify theft from the FTC or the following:
Washington D.C. Attorney General:
Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

GenRx™

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
TO THE PARENT OR GUARDIAN OF:
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear Parent or Guardian of <<Name 1>>,

GenRx Pharmacy ("GenRx") is writing to you as the parent or guardian of a minor GenRx patient. GenRx values our relationship with our patients and respects the security of your minor's information. We are writing to notify you about a data security incident we recently experienced and the steps we have taken in response. Although we are not aware of any actual harm to anyone as a result of this security incident, the cyberattack against GenRx did involve your minor's personal information. Please note, neither your minor's social security number nor any of your minor's financial information was involved. We recognize the concern this may cause, and we deeply regret that this incident occurred.

WHAT HAPPENED?
On September 28, 2020, GenRx found evidence of ransomware on our system and immediately began an investigation, including hiring independent information security and technology experts to assist with incident response and forensic investigation. In a ransomware attack, cybercriminals attempt to disrupt the business by locking the business out of its own data. During the ransomware attack against GenRx, we had full access to all data with unaffected backups, and we were able to maintain continuous business operations as we investigated.

Together with forensic experts, GenRx terminated the cybercriminal's access to GenRx systems the same day (September 28, 2020) and confirmed that an unauthorized third party deployed the ransomware only one day before (September 27, 2020). On November 11, 2020, we confirmed that the cybercriminal was able to remove a small number of files that included certain health information GenRx used to process and ship prescriptions.

WHAT INFORMATION WAS INVOLVED?
The cybercriminals accessed and removed the following health information about your minor: patient ID, transaction ID (a number generated to process the prescription, not related to your or your minor's financials), first and last name, date of birth, gender, medication list, health plan information (including member ID), and prescription information. **Please be assured that your minor's social security number and your minor's financial information were <u>not</u> affected. We do not collect your minor's SSN or maintain financial information, so there is no way that cybercriminals could access this information on GenRx systems.**

WHAT WE ARE DOING.
After becoming aware of this incident, we took prompt action to secure our system to help ensure that the cybercriminal no longer had access. The cybercriminal had access to our systems for only a few hours. In addition to our existing security measures, GenRx has upgraded firewall firmware, added additional anti-virus and web-filtering software, instituted multifactor authentication, increased Wi-Fi network traffic monitoring, provided additional training to employees, updated internal policies and procedures, and installed real-time intrusion detection and response software on all workstations and servers that access the company network. GenRx is also assessing further options to enhance our protocols and controls, technology, and training, including strengthening encryption.

WHAT YOU CAN DO.
While neither your minor's social security number nor your minor's financial information was affected, we wanted to provide you with some best practice recommendations. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your minor's account statements and monitoring free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to the financial institutions or company with which the account is maintained, as well as applicable authorities, including your state attorney general and the Federal Trade Commission. Please see the Attachment for additional resources.

FOR MORE INFORMATION.
For further information and assistance, please contact 877-835-1827 between 9am - 9pm Eastern Time, Monday through Friday.

Sincerely,

Richelle Aldrich
Executive Vice President, Architecture, Business Analytics & Operations
GenRx Pharmacy

ATTACHMENT FOR COLORADO, ILLINOIS, AND WASHINGTON, DC RESIDENTS
ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
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 *www.annualcreditreport.com*, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

You may also decide 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 for the purpose of requesting a copy of your credit report or for general information is listed here:

Equifax
1-800-685-1111
www.equifax.com/CreditReport Assistance
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com/fraud
P.O. Box 1000
Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze free of charge on your credit files and fraud alerts. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay 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 contact information listed above.

FOR WASHINGTON D.C. RESIDENTS
You can obtain information about preventing identify theft from the FTC or the following:
Washington D.C. Attorney General:
Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001