



Children's Choice Pediatrics

C/O ID Experts  
PO Box 4219  
Everett WA 98204

ENDORSE



Parent or Guardian of



NAME  
ADDRESS1  
ADDRESS2

SEQ  
CODE 2D  
Ver 2M

BREAK

December 16, 2019

Re: Data Security Incident

Dear Parent or Guardian of **SALUTATION**,

We are writing to inform you of a data security incident experienced by PediHealth, PLLC, dba Children's Choice Pediatrics ("Children's Choice") that may have involved your child's personal information. At Children's Choice we take the privacy and security of our patients' information very seriously. We are sending you this letter to notify you about the incident and provide information about steps you can take to help protect your child's personal information.

### What Happened?

On October 27, 2019, Children's Choice discovered it had been the victim of a ransomware attack. The impacted servers contained information for Children's Choice patients including names, addresses, and health information, including immunization records. The impacted servers did not and do not store Social Security numbers.

Upon learning of this incident, we immediately took steps to secure our computer system. In addition, we began an investigation to identify the affected individuals and the nature of affected information. We consulted information technology personnel and cybersecurity experts to assist us in our investigation, and with their help, we attempted to restore the impacted records. However, some patient records were unfortunately irretrievably deleted. We are unaware of the misuse of any of your child's personal information, but out of an abundance of caution, we are notifying you about this incident and providing you information about steps you can take to protect your child's personal information.

### What Information Was Involved?

Your child's name, address, phone number, date of birth, date(s) of service, prescriptions, immunization records, and treatment provider information may have been involved in the incident. Your child's Social Security number is not involved in the incident.

### What We Are Doing and What You Can Do.

Since discovering the incident, Children's Choice has taken steps to strengthen the security of personal information in its possession, in order to prevent similar incidents from occurring in the future. In addition, Children's Choice is providing you with information about steps that you can take to help protect your child's personal information.

In addition, while we are taking steps to recreate immunization records, as a result of the deletion of the impacted records, we are suggesting that our patients request a copy of their immunization records from any alternative source, maintain a copy for your records, and provide a copy to our office so that we can include the immunization record in our restored file.

**For More Information.**

We appreciate your patience and loyalty through this incident. If you have any questions, please call 1-833-918-2058 from 8:00 a.m. to 8:00 p.m., Central Time, Monday through Friday or visit <https://ide.myidcare.com/ccp> for more information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause.

Sincerely,

A handwritten signature in cursive script that reads "Cheryl Eley MD". The signature is written in black ink and is positioned above the printed name.

Cheryl Eley, MD  
Children's Choice Pediatrics

## Steps You Can Take to Further Protect Your Information

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant for the next twelve to twenty-four months and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the “FTC”).

**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/>, calling toll-free 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. If you detect any information related to fraudulent transactions, you should notify the credit reporting agency that issued the report and have it deleted. You can also contact one of the following three national credit reporting agencies:

<b>Equifax</b> P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 9532 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 1000 Chester, PA 19016 1-877-322-8228 <a href="http://www.transunion.com">www.transunion.com</a>	<b>Free Annual Report</b> P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 <a href="http://www.annualcreditreport.com">www.annualcreditreport.com</a>
--	---	---	---

**Fraud Alert:** 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 identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze:** In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You are encouraged to report suspected identity theft to the FTC. You may also report suspected identity theft to local law enforcement, including the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

<b>Federal Trade Commission</b> 600 Pennsylvania Ave, NW Washington, DC 20580 <a href="http://consumer.ftc.gov">consumer.ftc.gov</a> , and <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a> 1-877-438-4338	<b>Maryland Attorney General</b> 200 St. Paul Place Baltimore, MD 21202 <a href="http://oag.state.md.us">oag.state.md.us</a> 1-888-743-0023	<b>North Carolina Attorney General</b> 9001 Mail Service Center Raleigh, NC 27699 <a href="http://ncdoj.gov">ncdoj.gov</a> 1-877-566-7226	<b>Rhode Island Attorney General</b> 150 South Main Street Providence, RI 02903 <a href="http://www.riag.ri.gov">http://www.riag.ri.gov</a> 401-274-4400
---	---	---	--

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

**Personal Information of a Minor:** You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>



Children's Choice Pediatrics

C/O ID Experts  
PO Box 4219  
Everett WA 98204

ENDORSE



NAME

ADDRESS1

ADDRESS2

CSZ

BREAK



SEQ  
CODE 2D  
Ver 1A

December 16, 2019

Re: Data Security Incident

Dear **SALUTATION**,

We are writing to inform you of a recent data security incident experienced by PediHealth, PLLC, dba Children's Choice Pediatrics ("Children's Choice") that may have involved your personal information. At Children's Choice we take the privacy and security of our patients' information very seriously. We are sending you this letter to notify you about the incident and provide information about steps you can take to protect your personal information.

**What Happened?**

On October 27, 2019, Children's Choice discovered it had been the victim of a ransomware attack. The impacted servers contained information for Children's Choice patients including names, addresses, and health care treatment information. The impacted servers did not and do not store Social Security numbers.

Upon discovering this incident, we immediately took steps to secure our computer system. In addition, we began an investigation to identify the affected individuals and the nature of affected information. We consulted information technology personnel and cybersecurity experts to assist us in our investigation, and with their help, we attempted to restore the impacted records. However, some patient records were unfortunately irretrievably deleted. We are unaware of the misuse of any of your personal information, but out of an abundance of caution, we are notifying you about this incident and providing you information about steps you can take to protect your personal information.

**What Information Was Involved?**

Your name, address, phone number, date of birth, date(s) of service, balance information, prescriptions, immunization records, and treatment provider information may have been involved in the incident.

**What We are Doing And What You Can Do.**

Since discovering the incident, Children's Choice has taken steps to strengthen the security of personal information in its possession, in order to prevent similar incidents from occurring in the future. In addition, although we are not aware of any misuse of your information, we are providing you with this notification about the incident. The following pages provide information about steps you can take to protect your personal information as a precautionary measure.

In addition, while we are taking steps to recreate immunization records, as a result of the deletion of the impacted records, we are suggesting that our patients request a copy of their immunization records from any alternative source, maintain a copy for your records, and provide a copy to our office so that we can include the immunization record in our restored file.

**For More Information.**

We appreciate your patience and loyalty through this incident. If you have any questions, please call 1-833-918-2058 from 8:00 a.m. to 8:00 p.m., Central Time, Monday through Friday or visit <https://ide.myidcare.com/ccp> for more information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause.

Sincerely,

A handwritten signature in cursive script that reads "Cheryl Eley MD".

Cheryl Eley, MD  
Children's Choice Pediatrics

## Steps You Can Take to Further Protect Your Information

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant for the next twelve to twenty-four months and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

**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/>, calling toll-free 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. If you detect any information related to fraudulent transactions, you should notify the credit reporting agency that issued the report and have it deleted. You can also contact one of the following three national credit reporting agencies:

<b>Equifax</b> P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 9532 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 1000 Chester, PA 19016 1-877-322-8228 <a href="http://www.transunion.com">www.transunion.com</a>	<b>Free Annual Report</b> P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 <a href="http://www.annualcreditreport.com">www.annualcreditreport.com</a>
--	---	---	---

**Fraud Alert:** 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 identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze:** In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You are encouraged to report suspected identity theft to the FTC. You may also report suspected identity theft to local law enforcement, including the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

<b>Federal Trade Commission</b> 600 Pennsylvania Ave, NW Washington, DC 20580 <a href="http://consumer.ftc.gov">consumer.ftc.gov</a> , and <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a> 1-877-438-4338	<b>Maryland Attorney General</b> 200 St. Paul Place Baltimore, MD 21202 <a href="http://oag.state.md.us">oag.state.md.us</a> 1-888-743-0023	<b>North Carolina Attorney General</b> 9001 Mail Service Center Raleigh, NC 27699 <a href="http://ncdoj.gov">ncdoj.gov</a> 1-877-566-7226	<b>Rhode Island Attorney General</b> 150 South Main Street Providence, RI 02903 <a href="http://www.riag.ri.gov">http://www.riag.ri.gov</a> 401-274-4400
---	---	---	--

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

**Personal Information of a Minor:** You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>