Cove
Family & Sports Medicine

C/O ID Experts
PO Box 10444
Dublin, Ohio 43017-4044

[First Name] [Last Name]
[Address1] [Address2]
[City, State Zip]

June 13, 2017

Dear [first name]:

Thank you for allowing Cove Family and Sports Medicine ("Cove Medicine") to serve your healthcare needs. We take patient privacy seriously, and as part of that commitment, we are sending you this letter to make you aware of a recent data security incident that affected your personal information. Please read this letter carefully.

On April 14, 2017, Cove Medicine's computer system was infected by a ransomware virus that encrypted our electronic medical software containing our patients' medical records. The ransomware demanded monetary payment from Cove Medicine in order to decrypt the files and allow us to regain access to them. The encrypted medical records contained patient information, including names, dates of birth, social security numbers, addresses, patient identification numbers, prescription information, diagnosis information, procedure information, and time and date of treatment. Your information was included among the patient records encrypted by the ransomware virus.

Cove Medicine did not pay the ransom to the cyber criminals, but instead removed the virus by reinstalling the operating system on our server and then restoring the majority of our patient records from backup copies. The backup records, however, were partially encrypted as well and we currently have not been able to restore our internal notes for visits that have occurred in approximately the past two years. We believe we will be able to restore all other treatment records, and this will not impair our ability to provide care to our patients. In addition, subsequent scans of our computer system have shown no further indications of the ransomware or other malware. Our investigation also has not shown any indication of exfiltration of any patient records by the ransomware or any other unauthorized access to our computer system. However, out of an abundance of caution and because of our commitment to data security and privacy, we are notifying all of our patients about this incident.

While we are not aware of any access to your information by a person outside of Cove Medicine, there are some steps you can take to help protect against any potential misuse of your information. Please refer to the enclosed materials for additional information.

We are very sorry for any concern or inconvenience this incident has caused or may cause you. If you have any other questions or concerns that you would like to discuss, please call our dedicated, toll-free incident response hotline at 844-828-3239.

Sincerely,

Amy Carter, MD

Alicia Krichev, MD

Jonathan Krichev, MD

Additional Steps to Help Protect Your Information

1. **Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies listed below. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any incorrect information on your report, you should report it immediately to the credit reporting agency.

2. **Report suspected fraud.** You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

3. **Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating any credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.alerts.equifax.com	www.experian.com	www.transunion.com

   It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

4. **Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to $5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

5. **You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

   - **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
   - **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.
   - **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.
   - **North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com/, Telephone: 1-919-716-6400.
   - **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392
   - **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400
   - **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338)