



Todd Rowe, Partner
20 North Wacker
Suite 4120
Chicago, IL 60606
Tel.: 773.558.2363
trowe@constangy.com

August 12, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith and Prophete LLP (“Constangy”) represents Kootenai Health and its subsidiaries Kootenai Clinic, Kootenai Outpatient Surgery and Kootenai Outpatient Imaging (collectively “Kootenai Health”) in connection with an incident described in greater detail below. The purpose of this letter is to notify you, in accordance with Maryland data breach notification statute, that this incident may have affected the personal and/or protected information of 220 Maryland residents. Kootenai Health hereby reserves all rights and defenses in connection herewith.

1. Nature of Incident

On March 2, 2024, Kootenai Health became aware of unusual activity that disrupted access to certain IT systems. Upon discovering this activity, Kootenai Health took steps to secure its digital environment. Kootenai Health also engaged leading cybersecurity experts to assist with an investigation and to determine whether personal information may have been accessed or acquired without authorization. The investigation revealed that an unknown actor may have gained unauthorized access to certain data from the Kootenai Health network on or about February 22, 2024. Kootenai Health then worked to conduct a comprehensive review of the impacted data to determine what personal and/or protected health information was involved and to verify the affected information and mailing addresses for impacted individuals to ensure Kootenai Health had the most up to date contact information. This process was completed on August 1, 2024.

The information involved, if impacted, may have included individuals’ names along with their dates of birth, Social Security numbers, driver’s license or government-issued identification numbers, medical record numbers, medical treatment and condition information, medical diagnoses, medication information, and health insurance information.

2. Number of Maryland residents affected

Kootenai Health notified 220 Maryland residents of the incident via first class U.S. mail on August 12, 2024. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the incident

In response to the incident, Kootenai Health retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Kootenai Health implemented additional security measures to further harden its environment in an effort to prevent a similar event from occurring in the future. Kootenai Health also reported this incident to federal law enforcement and is cooperating with the investigation.

Kootenai Health is notifying the affected individuals and providing resources and steps individuals can take to help protect their information. In addition, Kootenai Health is offering affected individuals complimentary credit monitoring and identity protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 12 months of credit monitoring, CyberScan dark web monitoring, fully managed identity recovery services, and \$1 million in identity theft insurance coverage. IDX will also support a call center for at least 90 days to answer incident related questions.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at 773.558.2363 or trowe@constangy.com.

Very truly yours,



Todd Rowe of
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Consumer Notification Letter


Kootenai Health
Return Mail to IDX
PO Box 480149
Niles, IL 60714

<<First Name>> <<Last Name>> <<Suffix>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

August 12, 2024

Subject: Notice of Data <<Variable Text 1: Breach or Security Incident>>

Dear <<First Name>> <<Last Name>>:

Kootenai Health and its subsidiaries Kootenai Clinic, Kootenai Outpatient Surgery and Kootenai Outpatient Imaging (collectively “Kootenai Health”) are writing to inform you of a data security incident that may have involved your personal and/or protected health information. Kootenai Health is committed to maintaining the trust of our valued <<Variable Text 2: employees and their dependents / patients>>, and the privacy and security of all information in our possession is a top priority. That is why we are notifying you of the event and providing you with resources to help protect your information. We encourage you to read this letter carefully and to follow the steps outlined at the end of this letter on how to protect your personal information.

What Happened? On March 2, 2024, Kootenai Health became aware of unusual activity that disrupted access to certain IT systems. Upon discovering this activity, we took steps to secure our digital environment. We also engaged leading cybersecurity experts to assist with an investigation and to determine whether personal information may have been accessed or acquired without authorization. The investigation revealed that an unknown actor may have gained unauthorized access to certain data from the Kootenai Health network on or about February 22, 2024. Kootenai Health then worked to conduct a comprehensive review of the impacted data to determine what personal and/or protected health information was involved and to verify the affected information and mailing addresses for impacted individuals to ensure we had the most up to date contact information. This process was completed on August 1, 2024.

What Information Was Involved? The information involved if impacted may have included your name along with your date of birth, Social Security number, driver’s license or government-issued identification number, medical record number, medical treatment and condition information, medical diagnoses, medication information, and health insurance information.

What We Are Doing? As soon as we discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. We notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the responsible parties accountable, if possible.

Kootenai Health is also offering you the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX, A Zero Fox Company. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. To enroll scan the QR image, go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter or call 1-888-663-1581. The deadline to enroll in these services is November 7, 2024.

What You Can Do. We encourage you to enroll in the complimentary credit protection services we are offering. With this protection, IDX can help you resolve issues if your identity is compromised. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information. IDX Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday, excluding holidays. Please call the help line at 1-888-663-1581 and supply the specialist with your unique code listed above.

We apologize for any concern or inconvenience that this may cause and hope you will take advantage of the remediation services offered.

Very truly yours,

Kootenai Health
2003 Kootenai Health Way
Coeur d'Alene, Idaho 83814

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing 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 also should 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 (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 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

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 one year. 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: You have the right to put a security freeze on your credit file for up to one year at no cost. 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 fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Idaho Attorney General

Consumer Protection Division
954 W. Jefferson, 2nd Floor
Boise, ID 83702
ag.idaho.gov/consumer-protection/
1-800-432-3545

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
<https://www.marylandattorneygeneral.gov/>
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
<https://ag.ny.gov/resources/individuals/consumer-issues/technology>
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

Washington Attorney General

Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188
atg.wa.gov
1-800-551-4636

Blue Cross of Idaho Members: If you are a Blue Cross of Idaho member through Kootenai Health's employer-sponsored plan, you are eligible for free identity protection services through Experian. You can enroll in these services by visiting the Experian website directly at <http://experianidworks.com/bcidaho>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.