McDonald Hopkins
A business advisory and advocacy law firm®



McDonald Hopkins PLC
300 North LaSalle Street
Suite 1400
Chicago, IL 60654
P 1.312.280.0111
F 1.312.280.8232

**Emily A. Johnson**
Direct Dial: 312-642-1796
E-mail: ejohnson@mcdonaldhopkins.com

January 24, 2020

**VIA U.S. MAIL**

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

**Re: Beaumont Health – Incident Notification**

Dear Sir or Madam:

McDonald Hopkins LLC represents Beaumont Health ("Beaumont"). I write to provide notification concerning an incident that may affect the security of personal information of one (1) New Hampshire resident. Beaumont's investigation of this incident is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Beaumont does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On December 10, 2019, Beaumont discovered that an individual formerly employed by Beaumont accessed patient information without authorization and might have disclosed the information to a solicitor. The information that was accessed included the affected New Hampshire resident's full name, address, date of birth, phone number, email address, insurance information and Social Security number. The information accessed also included the reason why the affected individual came to Beaumont for medical care. No other financial information was accessed. It is believed that the solicitor works for a personal injury attorney, and that the personal injury attorney or the solicitor may have contacted the affected individual. Upon learning of this issue, Beaumont commenced a prompt and very thorough investigation. As part of its investigation, Beaumont has worked very closely with external cybersecurity professionals. The employee responsible for this incident is no longer employed by or affiliated with Beaumont.

Beaumont provided the affected resident with written notification of this incident commencing on or about January 24, 2020 in substantially the same form as the letter attached hereto. Beaumont provided the affected resident with twelve (12) months of complimentary credit monitoring as well as recommendations for steps to take to protect the affected resident's medical information.

At Beaumont, safeguarding personal information is a top priority. Beaumont is fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Beaumont continuously evaluates its practices and internal controls to enhance the security and privacy of personal information and will make changes, as necessary.

Notice is being provided pursuant to the HIPAA Breach Notification Rule, 45 CFR §§ 164.400, *et seq.*

Should you have any questions regarding this notification, please contact me at (312) 642-1798 or ejohnson@mcdonaldhopkins.com.

Sincerely,

Emily A. Johnson

Encl.

# Beaumont

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>>

***IMPORTANT INFORMATION***
***PLEASE REVIEW CAREFULLY***

<<Date>>

Dear <<Name1>>:

The privacy and security of the personal information we maintain is of the utmost importance to Beaumont Health ("Beaumont"). A recent incident might have involved some of your patient registration information. This letter provides information about the incident, explains the services we are providing to you, and explains how we protect your information.

*What Happened?*

We recently learned that an individual formerly employed by Beaumont accessed some patient information without authorization and might have disclosed the information to a solicitor. We believe this solicitor works for a personal injury attorney. The personal injury attorney or solicitor might have contacted you.

*What We Are Doing.*

Upon learning of this issue, we launched an investigation. As part of our investigation, we have worked closely with the State of Michigan's Attorney Grievance Commission. We discovered on December 10, 2019 that the information the former employee accessed contained some of your protected health information. The employee was terminated. Beaumont Health will work closely with law enforcement should they seek to prosecute this former employee.

*What Information Was Involved.*

The information accessed contained some of your protected health information, including your full name, address, date of birth, phone number, email address, insurance information, and Social Security number. The information accessed also included the reason why you came to Beaumont Health for medical care. No other financial information was accessed.

*What You Can Do.*

To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis. To the extent it is helpful, we have also provided information on protecting your medical information on the following pages.

*For More Information.*

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

**If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 866-977-0774.** This response line is staffed with professionals familiar with this incident and knowledgeable about what you can do to protect your information. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. EST.

Sincerely,

Privacy Officer
Beaumont Health

## – OTHER IMPORTANT INFORMATION –

**1. Enrolling in Complimentary 12-Month Credit Monitoring.**

**Activate IdentityWorks Credit 3B Now in Three Easy Steps**

1. ENROLL by: **<<Enrollment Deadline>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: https://www.experianidworks.com/3bcredit
3. PROVIDE the **Activation Code**: **<<Enrollment Code>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **<<Engagement Number>>** as proof of eligibility for the identity restoration services by Experian.

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian, Equifax, and TransUnion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at https://www.experianidworks.com/3bcredit or call 877-288-8057 to register with the Activation Code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## 2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

**Equifax**
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

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

**TransUnion LLC**
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

## 3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

**Equifax Security Freeze**
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com/personal/
credit-report-services/credit-freeze
1-800-349-9960

**Experian Security Freeze**
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

**TransUnion Security Freeze**
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

## 4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

## 5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

## 6. Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement," which you receive from your health insurance company. Follow up with your insurance company or care provider regarding any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider regarding any items you do not recognize.