McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

September 18, 2017

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: AU Medical Center, Inc./Augusta University – Incident Notification

Dear Attorney General Foster:

McDonald Hopkins PLC represents AU Medical Center, Inc. ("AUMC") and Augusta University. I write to provide notification concerning an incident that may affect the security of personal information of one (1) New Hampshire resident. AUMC and Augusta University's investigation 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, AUMC and Augusta University do not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

AUMC and Augusta University learned that a limited number of medical faculty at Augusta University were victims of a phishing attack to their email system. Upon learning of the issue, Augusta University promptly disabled the impacted email accounts and required password changes for the compromised accounts and maintained heightened monitoring of the accounts to ensure that no other suspicious activity was taking place. In addition, Augusta University commenced an investigation into the incident and retained an independent computer forensic firm to analyze the extent of any compromise to the email accounts and the security of the emails and attachments contained within them.

Since completing the forensic investigation and comprehensive manual document review, on July 18, 2017, the forensic investigation concluded that an unauthorized third party accessed members of the medical faculty email accounts containing protected health information of less than 1% of AUMC's patient population. The investigation further determined that the compromise of the email accounts occurred during a limited period of time from April 20, 2017 to April 21, 2017, but the forensic firm could not definitively conclude if information was actually accessed, viewed, downloaded or otherwise acquired by the unauthorized user.

AUMC and Augusta University confirmed that the compromised email accounts contained patient full name and either one or more of the following: address, date of birth, Social Security number, medical record number, insurance information, prescription information,

diagnosis/condition, and/or treatment information. A limited number of driver's license numbers and financial account numbers were involved for residents of other states.

AUMC and Augusta University wanted to make you (and the affected resident) aware of the incident and explain the steps AUMC and Augusta University are taking to help safeguard the resident against identity fraud. AUMC and Augusta University provided the New Hampshire resident with written notice of this incident commencing on September 15, 2017, in substantially the same form as the letter attached hereto. AUMC and Augusta University offered the resident complimentary credit monitoring services and have advised the resident to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. AUMC and Augusta University have advised the resident about the process for placing a fraud alert on credit files, placing a security freeze, and obtaining a free credit report. The resident also has been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

AUMC and Augusta University take its obligation to help protect personal information very seriously. AUMC and Augusta University are continually evaluating and modifying practices to enhance appropriate security and privacy measures, including ongoing cybersecurity awareness of their workforce.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,

James J. Giszczak

Encl.

Health
AUGUSTA UNIVERSITY
Return Mail Processing Center
PO 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 <<Name1>>:

The privacy of your personal information is of the utmost importance to AU Medical Center, Inc. ("AUMC") and Augusta University. AUMC is the academic medical center affiliated with Augusta University. We are writing to provide you with important information about a recent incident involving some of your protected health information that you supplied to AUMC. We want to provide you with information regarding the incident and let you know that we continue to take significant measures to protect your information.

We learned that a limited number of our medical faculty at Augusta University were victims of a phishing attack to our email system. Phishing attacks are carried out using emails sent from unknown sources that appear to be legitimate that request personally identifiable information, protected health information, or other confidential information. Upon learning of the issue, Augusta University promptly disabled the impacted email accounts and required password changes for the compromised accounts and maintained heightened monitoring of the accounts to ensure that no other suspicious activity was taking place. In addition, Augusta University simultaneously commenced an investigation into the incident and retained an independent computer forensic firm to analyze the extent of any compromise to the email accounts and the security of the emails and attachments contained within them.

Since completing our investigation and manual document review, on July 18, 2017, we concluded that an unauthorized third party accessed two medical faculty email accounts containing your protected health information. The forensic investigation further determined that the compromise of the email accounts occurred during a limited period of time from April 20, 2017 to April 21, 2017, but the forensic firm could not definitively conclude if your information was ***actually*** accessed, viewed, downloaded or otherwise acquired by the unauthorized user.

Further, based on the investigation conclusion, we have devoted considerable time and effort to determine what information was contained in the affected email accounts. We can confirm that the compromised email accounts contained your full name and either one or more of the following: your Social Security number, date of birth, home address, medical record number, insurance information, prescription information, diagnosis/condition, and/or treatment information. Your financial account information was **not** contained in the compromised accounts.

To date, we are not aware of improper use of your information. Due to the complexity of the intrusion, however, we cannot conclusively determine whether the unauthorized user actually acquired or viewed any of your information. Out of an abundance of caution, we wanted to make you aware of the incident. In addition, to protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks^{SM} 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, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. To the extent it is helpful, we have provided steps you can take to protect your health information.

On behalf of AUMC and Augusta University, please accept our sincere apologies that this incident occurred. We are committed to maintaining the privacy of AUMC patient information, and we continually evaluate and modify our practices to enhance appropriate security and privacy measures, including ongoing cybersecurity awareness of our workforce.

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 888-398-6850. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

C Adams

Christine Adams, CHC, CHPC
Enterprise Privacy Officer
AU Medical Center, Inc.
Augusta University

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

To help protect your identity, 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 superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<**Enrollment date**>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **www.protectmyid.com/alert**
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/3bcreditone
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.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "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. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111
1-800-349-9960 (NY residents only)

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

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.

If you live in ***North Carolina***, in addition to the FTC, the North Carolina Office of the Attorney General can also be contacted to obtain information on the steps you can take to prevent identity theft:

North Carolina Department of Justice
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Instances of known or suspected identity theft should also be reported to law enforcement.

6. Protecting Your Health Information.

We have no information to date indicating that your Protected Health Information (PHI) involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from 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 for 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 for any items you do not recognize.