McDonald Hopkins
A business advisory and advocacy law firm®

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

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

November 17, 2017

VIA E-MAIL: *SecurityBreach@atg.wa.gov*

Office of the Washington State Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: The Medical College of Wisconsin, Inc. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents The Medical College of Wisconsin, Inc. ("MCW"). I write to provide notification concerning an incident that may affect the security of personal information of six (6) Washington residents. MCW'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, MCW does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

MCW recently learned that a limited number of its employees were victims of a sophisticated spear-phishing attack to MCW's email system. Upon learning of the issue, MCW promptly disabled the impacted email accounts, changed the passwords to those accounts and maintained heightened monitoring of the accounts to ensure that no other suspicious activity was taking place. In addition, MCW 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 the forensic investigation and comprehensive manual document review, on September 20, 2017, the forensic investigation concluded that an unauthorized third party accessed a limited number of email accounts belonging to MCW employees. The investigation further determined that the compromise of the email accounts occurred between July 21, 2017 and July 28, 2017, but the forensic firm could not definitively conclude what information within the accounts, if any, was actually accessed, viewed, downloaded or otherwise acquired by the unauthorized user.

MCW has confirmed that the compromised email accounts contained either one or more of the following: residents' names, dates of birth, home addresses, medical record numbers, health insurance information, date(s) of service, surgical information, diagnosis/condition, and/or treatment information. In addition, the Social Security number of one (1) Washington resident

was contained within the email accounts at issue. MCW has no evidence to suggest that any other personal information belonging to the Washington residents was involved in this incident.

To date, MCW has not received any reports of identity fraud, theft or improper use of the residents' information as a direct result of this incident. Nevertheless, MCW wanted to make you (and the affected residents) aware of the incident and explain the steps MCW is taking to help safeguard the residents safeguard the residents against potential misuse of their information. MCW provided the Washington residents with written notice of this incident commencing on November 17, 2017, in substantially the same form as the letter attached hereto. As a precautionary measure, MCW is offering a complimentary one-year membership of credit monitoring and identity theft protection services to the Washington resident whose Social Security number was involved in this incident. This resident also has been provided with best practices to protect their personal information, such as placing a fraud alert and/or security freeze on their credit files and obtaining a free credit report, as well as the contact information for the consumer reporting agencies and the Federal Trade Commission. MCW has advised the residents to remain vigilant in reviewing their financial account statements for fraudulent or irregular activity on a regular basis. In addition, MCW is providing all affected residents with best practices to protect their health information and is also providing dedicated call center support to answer questions.

MCW is committed to maintaining the privacy of patient information and continually evaluating and modifying its practices and procedures to enhance appropriate security and privacy measures to prevent recurrence of this incident, including conducting ongoing cyber awareness training for its workforce and regularly updating its system security and firewalls.

In addition to notifying the Washington State Attorney General's Office, as required pursuant to RCW 19.255.010(10) and (15), MCW notified the Secretary of the U.S. Department of Health and Human Services on November 17, 2017, as required by the rules implementing the federal Health Insurance Portability and Accountability Act.

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

Sincerely,

James J. Giszczak

JJG/sdg
Encl.

MEDICAL COLLEGE OF WISCONSIN

[redacted]

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>:

I am writing to provide you with important information about a recent incident involving the security of some of your personal information that you supplied to us at affiliated hospitals or clinics as a result of the services we provided to you. We wanted to provide you with information regarding the incident and let you know that we continue to take significant measures to protect your information. The privacy of your personal information is of utmost importance to the Medical College of Wisconsin ("MCW").

As a large organization, MCW is often the target of hackers and scammers looking to steal information through "phishing" and "spear phishing." Phishing is defined as the activity of defrauding an online account holder of institutional, financial or personal information by posing as a legitimate company, organization or individual through the use of email. Spear phishing is an email targeting a specific individual, organization, or business sent to a very small number of individuals to avoid detection.

We recently learned that a limited number of our employees at MCW were victims of a spear phishing attack to our email system. Upon learning of the issue, we promptly disabled the impacted email accounts, changed the passwords to those accounts and maintained heightened monitoring of the accounts to ensure that no other suspicious activity was taking place. In addition, we simultaneously commenced an investigation of 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 September 20, 2017, we concluded that an unauthorized third party accessed a limited number of email accounts belonging to MCW employees. The forensic investigation further determined that the compromise of the email accounts occurred between July 21, 2017 and July 28, 2017, but the forensic firm could not definitively conclude what information within the accounts, if any, was ***actually*** accessed, viewed, downloaded or otherwise acquired by the unauthorized user.

Further, based on the investigation conclusions, we have devoted considerable time and effort to determine what information was contained in the affected email accounts. We conducted a sophisticated review of each email and attachment contained within the impacted email accounts that was forensically identified as having contained personal or protected health information to ensure accuracy and confirm those potentially impacted. Based on our review, we can confirm that the compromised email accounts contained either one or more of the following: your name, date of birth, home address, medical record number, health insurance information, date(s) of service, surgical information, diagnosis/condition, and/or treatment information. In addition, your Social Security number *may* have been contained within the compromised email accounts.

To date, we are not aware of any reports of identity fraud, theft or improper use of your information as a direct result of this incident. 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 and explain the services we are making available to safeguard you against identity fraud.

Enclosed in this letter you will find information on enrolling in 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. Also enclosed you will find information about other precautionary measures you can take to protect your personal information, including obtaining a free credit report and placing a Fraud Alert and/or Security Freeze on your credit files. 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 the following pages.

On behalf of MCW, please accept our apology that this incident occurred. We are committed to maintaining the privacy of our patients' information and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of our patients' 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 [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against potential misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.

Sincerely,

[redacted]

[redacted]

Medical College of Wisconsin

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring and Identity Protection Services.

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 Deadline>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [redacted]
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 [redacted]. 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 [redacted]
or call [redacted] 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 [redacted] 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 [redacted].

* 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. Alternatively, you may file the Fraud Alert online. Here is a link to the Experian fraud alert home page: https://www.experian.com/fraud/center.html

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-888-766-0008
www.equifax.com

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

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

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
1-800-685-1111
https://www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze (FVAD)
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
https://freeze.transunion.com/

Please note that there may be a charge associated with placing, temporarily lifting, or removing a security freeze with each of the above credit reporting companies. These fees vary by state, so please call or visit the credit reporting agencies' websites to find out the specific costs applicable to the State in which you currently reside.

If you decide to place a Security Freeze on your credit file, *in order to do so without paying a fee*, you will need to send a copy of a valid identity theft report or police report, by mail, to each credit reporting company to show that you are a victim of identity theft and are eligible for free security freeze services. 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.

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.

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and monitoring free credit reports for any unauthorized activity. 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 believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC and/or the Attorney General's office in your state. You can obtain information from these sources about the steps individuals can take to protect themselves from identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. This notice has not been delayed by law enforcement.

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 https://www.identitytheft.gov/, by phone at 1-877-IDTHEFT (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.

6. Reporting Identity Fraud to the IRS.

If you believe you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you do the following:

- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf.
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police or law enforcement department.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

7. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

8. 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.