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

August 30, 2018

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Augusta University – Incident Notification

Dear Attorney General Delaney:

McDonald Hopkins PLC represents Augusta University. I write to provide notification concerning an incident that may affect the security of personal information of fourteen (14) New Hampshire residents. Augusta University's investigation is ongoing and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Augusta University does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Augusta University was targeted by a series of fraudulent emails. These sophisticated "phishing" emails solicited user names and passwords, giving hackers access to a small number of internal email accounts. Upon recognizing the nature of the attack, Augusta University acted promptly to stop the intrusion: disabling the impacted email accounts, requiring password changes for the compromised accounts, and maintaining 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 engaged external cybersecurity professionals to analyze the extent of any compromise to the email accounts and the security of the emails and attachments contained within. On July 31, 2018, investigators determined that email accounts accessed earlier by an unauthorized user may have given them access to personal and/or protected health information. The investigation also determined that the incident occurred on September 10-11, 2017.

Individual information that may have been in compromised email accounts included names and one or more of the following: addresses, dates of birth, medical record numbers, medical information, treatment information, surgical information, diagnoses, lab results, medications, dates of service and/or insurance information. For some individuals, information may have included a Social Security number and/or driver's license number. For a limited number of individuals, information may also have included payment card or bank account numbers.

Additionally, in response to this incident, Augusta University has or will be promptly initiating several actions to protect against future incidents, including: installing new leadership in a number of critical areas; implementing multifactor authentication for off-campus email and system access; reviewing and adopting of solutions to limit email retention; implementing policy and procedure changes regarding protected health information in email communications; employing software to screen emails for protected health information or personally identifiable information to prevent them from sending; increasing employee training on their critical role in preventing security breaches; and enhancing compliance-related policies and procedures.

Augusta University is providing written notification via U.S. Mail commencing on August 30, 2018 to individuals impacted by this incident (where last known home address was available), in substantially the same form as the letter attached hereto. Where applicable, Augusta will offer free credit monitoring services for one year to individuals whose Social Security number was included in the compromised email accounts. Augusta will advise the residents to remain vigilant in reviewing account and explanation of benefits statements for fraudulent or irregular activity. Augusta will provide dedicated call center support to answer questions. Where applicable, Augusta will advise the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. Where applicable, the residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

In addition, we have notified the Secretary of the U.S. Department of Health and Human Services Office for Civil Rights, pursuant to 45 CFR 164.408.

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

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 <<Name 1>>:

At Augusta University, our top priorities are our students, employees and our patients, and that includes our obligation to safeguard their personal and health information.

We regret to inform you that a phishing attack on Augusta University's email accounts may have led to the unauthorized access of protected health information and other personal information. The university has been working closely with external cybersecurity professionals to define the scope of this incident.

What Happened?

Augusta University was targeted by a series of fraudulent emails. These sophisticated "phishing" emails solicited user names and passwords, giving hackers access to a small number of internal email accounts.

Upon recognizing the nature of the attack, we acted promptly to stop the intrusion: disabling the impacted email accounts, requiring password changes for the compromised accounts, and maintaining heightened monitoring of the accounts to ensure that no other suspicious activity was taking place.

On July 31, 2018, investigators determined that email accounts accessed earlier by an unauthorized user may have given them access to your personal and/or protected health information. The investigation also determined that the incident occurred on September 10-11, 2017.

What information was included?

Based on our review, data including your name and one or more of the following was contained in the email accounts that were accessed: your address, date of birth, driver's license number, medical record number, medical information, treatment information, surgical information, diagnoses, lab results, medications, dates of service and/or insurance information. Your Social Security number was not contained in the compromised accounts.

What We Have Done.

We deeply regret this incident and the concern it has caused our students, employees and patients. In response, we have or will be promptly initiating several actions to protect against future incidents, including:

- Installing new leadership in a number of critical areas
- Implementing multifactor authentication for off-campus email and system access
- Review and adoption of solutions to limit email retention
- Implementing policy and procedure changes regarding protected health information in email communications
- Employing software to screen emails for protected health information or personally identifiable information to prevent them from sending
- Increasing employee training on their critical role in preventing security breaches
- Enhancing our compliance-related policies and procedures

What Can I Do?

We encourage you to remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. Below is information about other precautionary measures you can take to protect your health information.

Where can I find more information?

If you have any questions or concerns 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 patients can do to protect against misuse of their information. The response line is available Monday through Friday, 9 a.m. to 9 p.m. Eastern Time.

Sincerely,

[redacted]

AU Medical Center, Inc.
Augusta University

– PRIVACY SAFEGUARDS INFORMATION –

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 patients 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.
- Remain vigilant in reviewing your account statements regularly for fraudulent or irregular activity.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Health
AUGUSTA UNIVERSITY
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

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 <<Name 1>>:

At Augusta University, our top priorities are our students, employees and our patients, and that includes our obligation to safeguard their personal and health information.

We regret to inform you that a phishing attack on Augusta University's email accounts may have led to the unauthorized access of protected health information and other personal information. The university has been working closely with external cybersecurity professionals to define the scope of this incident.

What Happened?

Augusta University was targeted by a series of fraudulent emails. These sophisticated "phishing" emails solicited user names and passwords, giving hackers access to a small number of internal email accounts.

Upon recognizing the nature of the attack, we acted promptly to stop the intrusion: disabling the impacted email accounts, requiring password changes for the compromised accounts, and maintaining heightened monitoring of the accounts to ensure that no other suspicious activity was taking place.

On July 31, 2018, investigators determined that email accounts accessed earlier by an unauthorized user may have given them access to your personal and/or protected health information. The investigation also determined that the incident occurred on September 10-11, 2017.

What information was included?

Based on our review, data including your name, Social Security number, and one or more of the following was contained in the email accounts that were accessed: your address, date of birth, driver's license number, medical record number, medical information, treatment information, surgical information, diagnoses, lab results, medications, dates of service and/or insurance information.

What We Have Done.

We deeply regret this incident and the concern it has caused our students, employees and patients. In response, we have or will be promptly initiating several actions to protect against future incidents, including:

- Installing new leadership in a number of critical areas
- Implementing multifactor authentication for off-campus email and system access
- Review and adoption of solutions to limit email retention
- Implementing policy and procedure changes regarding protected health information in email communications
- Employing software to screen emails for protected health information or personally identifiable information to prevent them from sending
- Increasing employee training on their critical role in preventing security breaches
- Enhancing our compliance-related policies and procedures

What Can I Do?

We want to help protect you from potential misuse of your personal information. We are offering you a free one-year membership for credit monitoring through Experian IdentityWorks℠ Credit 3B. This service 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 one-year membership, please see the additional information provided in this letter.

We encourage you to remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. Below is information about other precautionary measures you can take, including placing a fraud alert and/or security freeze on credit files and obtaining a free credit report. Finally, we want to make you aware of what you can do to protect your medical identity by monitoring your health information.

Where can I find more information?

If you have any questions or concerns 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 patients can do to protect against misuse of their information. The response line is available Monday through Friday, 9 a.m. to 9 p.m. Eastern Time. Information is also available on our website at www.augusta.edu/notice.

Sincerely,

[redacted]

AU Medical Center, Inc.
Augusta University

– PRIVACY SAFEGUARDS INFORMATION –

1. 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 patients 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.
- Remain vigilant in reviewing your account statements regularly for fraudulent or irregular activity.

2. Enrolling in Complimentary 12-Month 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: [redacted]
3. PROVIDE the **Activation Code**: <<Activation 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.

* 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.

Activate your membership today at https://www.experianidworks.com/3bcredit
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 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 [redacted].

3. Placing a Fraud Alert

You may 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	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

4. 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	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	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 monitoring 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.

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.

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. After you sign up for the credit monitoring service, you may refreeze your credit file. We encourage you to wait to place a security freeze on your credit file until you have enrolled in the credit monitoring service to avoid paying additional fees related to placing an initial security freeze on your credit file, temporarily lifting or removing the security freeze and subsequently refreezing your credit file.

5. 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.

6. 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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: 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.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity;
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
4. Payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392