EXHIBIT A

PHYSICIANS

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

University of Minnesota Physicians ("UMPhysicians") is writing to make you aware of a data security event that potentially affected the confidentiality of some of your personal information. We have no evidence to suggest that your information was actually viewed during this event and we are not aware of any attempted or actual misuse of your information. However, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? UMPhysicians identified that cyber attackers used phishing emails to fraudulently access two employee email accounts. The two phishing email attacks were identified on January 31, 2020 and February 4, 2020, shortly after they occurred. UMPhysicians took immediate steps to secure the email accounts and began working with third-party computer forensic investigators to determine the nature and scope of the incidents. The investigation indicated that an unknown actor had access to one employee email account on January 30 and January 31, 2020, and another employee email account on February 4, 2020, for a brief period of time.

Unfortunately, the investigation was unable to determine with certainty to what extent any emails within the two email accounts may have been viewed by the cyber attackers. Based on this, in an abundance of caution, we worked with third-party specialists to perform a comprehensive review of all information stored in the email accounts at the time of the incidents to identify any personal information present in the email accounts. The employee email accounts contained information about individuals because the email accounts were used to perform normal business operations related to health care services provided by UMPhysicians. Upon completion of the third-party specialists' review of the full contents of the email accounts, which was a detailed and lengthy process that involved multiple steps to identify the relevant data, we immediately began assessing the results to confirm the identities of potentially affected individuals and obtain their current mailing addresses or other contact information. We recently completed this comprehensive review process.

What Information Was Involved? Our review determined that an email message containing the following types of information relating to you was present in an affected email account during this incident: <<b2b_text_1 (Data Impacted)>>. We have no evidence indicating that your information was actually viewed during the incident or has been copied or otherwise misused. However, the perpetrators did have access to the two email accounts for a limited period of time so it is possible they may have seen some of your information.

What We Are Doing. UMPhysicians takes this incident and the security of the information in its care very seriously. We quickly identified the attacks and took steps to secure the affected email accounts. At the time of the attacks, UMPhysicians had multiple email security controls in place, including multi-factor authentication. We also require all employees to participate in privacy and security training, and we regularly conduct exercises to try to make sure personnel do not fall prey to phishing and related scams. As part of our ongoing commitment to the privacy and security of personal information in our care, we reviewed our policies and procedures and implemented additional safeguards to further control and secure the information in our email system. For example, we conducted refresher training for personnel related to best practices in identifying phishing attempts, and we implemented restrictions on email retention. We also purchased additional technology that will provide for more enhanced detection and prevention of phishing emails. In addition, we notified state and federal regulators where we are required to do so. Further, while we are unaware of any misuse of your information as a result of this incident, we are offering you access to complimentary identity monitoring services for 12 months through Kroll.

What You Can Do. You can learn more about accessing complimentary identity monitoring through Kroll and find out more about how to help protect against potential identity theft and fraud in the enclosed Steps You Can Take to Help Protect Your Personal Information. We encourage you to remain vigilant against incidents of identity theft by reviewing your account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company or health care provider.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-???-???-????, Monday through Friday (except U.S. holidays), during the hours of 8:00 a.m. to 5:30 p.m., Central Time. You may also write to University of Minnesota Physicians at 720 Washington Avenue SE Suite #200, Minneapolis, MN 55414; Attention: Compliance Officer.

We are very sorry this incident occurred and sincerely regret any inconvenience or concern it may

cause.

Sincerely,

Sara DeSanto
Compliance Officer
University of Minnesota Physicians

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Activation Instructions

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://[IDMonitoringURL]** to activate and take advantage of your identity monitoring services.

*You have until **[Date]** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

If you find suspicious activity on your credit reports or have reason to believe your information has been misused, the Federal Trade Commission encourages you to file a report with its Fraud Department. Your report will be added to the FTC's Identity Theft Data Clearinghouse. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. You also have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

For Maryland residents: The Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; and www.oag.state.md.us.

For North Carolina residents: The Attorney General may be contacted at 9001 Mail Service Center, Raleigh; NC 27699-9001, 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents: The Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [x] Rhode Island residents impacted by this incident.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and https://ag.ny.gov/.

For Washington, D.C. residents: The Attorney General may be contacted at: Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001; (202) 727-3400; and www.oag@dc.gov.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

PHYSICIANS

<<Date>> (Format: Month Day, Year)

Parents of
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear Parents of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

University of Minnesota Physicians ("UMPhysicians") is writing to make you aware of a data security event that potentially affected the confidentiality of some of your minor child's personal information. We have no evidence to suggest that your minor child's information was actually viewed during this event and we are not aware of any attempted or actual misuse of your minor child's information. However, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? UMPhysicians identified that cyber attackers used phishing emails to fraudulently access two employee email accounts. The two phishing email attacks were identified on January 31, 2020 and February 4, 2020, shortly after they occurred. UMPhysicians took immediate steps to secure the email accounts and began working with third-party computer forensic investigators to determine the nature and scope of the incidents. The investigation indicated that an unknown actor had access to one employee email account on January 30 and January 31, 2020, and another employee email account on February 4, 2020, for a brief period of time.

Unfortunately, the investigation was unable to determine with certainty to what extent any emails within the two email accounts may have been viewed by the cyber attackers. Based on this, in an abundance of caution, we worked with third-party specialists to perform a comprehensive review of all information stored in the email accounts at the time of the incidents to identify any personal information present in the email accounts. The employee email accounts contained information about individuals because the email accounts were used to perform normal business operations related to health care services provided by UMPhysicians. Upon completion of the third-party specialists' review of the full contents of the email accounts, which was a detailed and lengthy process that involved multiple steps to identify the relevant data, we immediately began assessing the results to confirm the identities of potentially affected individuals and obtain their current mailing addresses or other contact information. We recently completed this comprehensive review process.

What Information Was Involved? Our review determined that an email message containing the following types of information relating to your minor child was present in an affected email account during this incident: <<b2b_text_1 (Data Impacted)>>. We have no evidence indicating that your minor child's information was actually viewed during the incident or has been copied or otherwise misused. However, the perpetrators did have access to the two email accounts for a limited period of time so it is possible they may have seen some of your minor child's information.

What We Are Doing. UMPhysicians takes this incident and the security of the information in its care very seriously. We quickly identified the attacks and took steps to secure the affected email accounts. At the time of the attacks, UMPhysicians had multiple email security controls in place, including multi-factor authentication. We also require all employees to participate in privacy and security training, and we regularly conduct exercises to try to make sure personnel do not fall prey to phishing and related scams. As part of our ongoing commitment to the privacy and security of personal information in our care, we reviewed our policies and procedures and implemented additional safeguards to further control and secure the information in our email system. For example, we conducted refresher training for personnel related to best practices in identifying phishing attempts, and we implemented restrictions on email retention. We also purchased additional technology that will provide for more enhanced detection and prevention of phishing emails. In addition, we notified state and federal regulators where we are required to do so. Further, while we are unaware of any misuse of your minor child's information as a result of this incident, we are offering you access to complimentary Minor Monitoring services for 12 months through Kroll.

What You Can Do. You can learn more about accessing complimentary Minor Monitoring through Kroll and find out more about how to help protect against potential identity theft and fraud in the enclosed Steps You Can Take to Help Protect Your Minor Child's Personal Information. We encourage you to remain vigilant against incidents of identity theft by reviewing your minor child's account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company or health care provider.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-???-???-????, Monday through Friday (except U.S. holidays), during the hours of 8:00 a.m. to 5:30 p.m., Central Time. You may also write to University of Minnesota Physicians at 720 Washington Avenue SE Suite #200, Minneapolis, MN 55414; Attention: Compliance Officer.

We are very sorry this incident occurred and sincerely regret any inconvenience or concern it may

cause.

Sincerely,

Sara DeSanto
Compliance Officer
University of Minnesota Physicians

STEPS YOU CAN TAKE TO HELP PROTECT YOUR MINOR CHILD's PERSONAL INFORMATION

Activation Instructions

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Visit **https://[IDMonitoringURL]** to activate and take advantage of your Minor Identity Monitoring services.

*You have until **[Date]** to activate your Minor Identity Monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your minor child's account statements, and to monitor your minor child's credit reports for suspicious activity and to detect errors.

While minors under the age of 18 typically do not have credit files, the following information relates to protecting one's credit once established. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

If you find suspicious activity on your credit reports or have reason to believe your information has been misused, the Federal Trade Commission encourages you to file a report with its Fraud Department. Your report will be added to the FTC's Identity Theft Data Clearinghouse. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. You also have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

For Maryland residents: The Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; and www.oag.state.md.us.

For North Carolina residents: The Attorney General may be contacted at 9001 Mail Service Center, Raleigh; NC 27699-9001, 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents: The Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [x] Rhode Island residents impacted by this incident.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and https://ag.ny.gov/.

For Washington, D.C. residents: The Attorney General may be contacted at: Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001; (202) 727-3400; and www.oag@dc.gov.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF MINOR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Minor Identity Monitoring. Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation . You have unlimited access to consultation with a Kroll fraud specialist. Support includes interpreting how personal information is accessed and used, explaining your rights and protections under the law, assistance with fraud alerts, and showing you the most effective ways to protect personal information, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration . An experienced Kroll licensed investigator will work on your behalf to resolve issues related to identity theft. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator will be able to dig deep to uncover all aspects of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

PHYSICIANS

<<Date>> (Format: Month Day, Year)

Estate of
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

To the Estate of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

University of Minnesota Physicians ("UMPhysicians") is writing to make you aware of a data security event that potentially affected the confidentiality of some of your deceased loved one's personal information. We have no evidence to suggest that your deceased loved one's information was actually viewed during this event and we are not aware of any attempted or actual misuse of your loved one's information. However, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? UMPhysicians identified that cyber attackers used phishing emails to fraudulently access two employee email accounts. The two phishing email attacks were identified on January 31, 2020 and February 4, 2020, shortly after they occurred. UMPhysicians took immediate steps to secure the email accounts and began working with third-party computer forensic investigators to determine the nature and scope of the incidents. The investigation indicated that an unknown actor had access to one employee email account on January 30 and January 31, 2020, and another employee email account on February 4, 2020, for a brief period of time.

Unfortunately, the investigation was unable to determine with certainty to what extent any emails within the two email accounts may have been viewed by the cyber attackers. Based on this, in an abundance of caution, we worked with third-party specialists to perform a comprehensive review of all information stored in the email accounts at the time of the incidents to identify any personal information present in the email accounts. The employee email accounts contained information about individuals because the email accounts were used to perform normal business operations related to health care services provided by UMPhysicians. Upon completion of the third-party specialists' review of the full contents of the email accounts, which was a detailed and lengthy process that involved multiple steps to identify the relevant data, we immediately began assessing the results to confirm the identities of potentially affected individuals and obtain their current mailing addresses or other contact information. We recently completed this comprehensive review process.

What Information Was Involved? Our review determined that an email message containing the following types of information relating to your loved one was present in an affected email account during this incident: <<b2b_text_1 (Data Impacted)>>. We have no evidence indicating that your loved one's information was actually viewed during the incident or has been copied or otherwise misused. However, the perpetrators did have access to the two email accounts for a limited period of time so it is possible they may have seen some of your loved one's information.

What We Are Doing. UMPhysicians takes this incident and the security of the information in its care very seriously. We quickly identified the attacks and took steps to secure the affected email accounts. At the time of the attacks, UMPhysicians had multiple email security controls in place, including multi-factor authentication. We also require all employees to participate in privacy and security training, and we regularly conduct exercises to try to make sure personnel do not fall prey to phishing and related scams. As part of our ongoing commitment to the privacy and security of personal information in our care, we reviewed our policies and procedures and implemented additional safeguards to further control and secure the information in our email system. For example, we conducted refresher training for personnel related to best practices in identifying phishing attempts, and we implemented restrictions on email retention. We also purchased additional technology that will

provide for more enhanced detection and prevention of phishing emails. In addition, we notified state and federal regulators where we are required to do so. Further, while we are unaware of any misuse of your loved one's information as a result of this incident, we are offering you access to complimentary Fraud Consultation and Identity Theft Restoration services for 12 months through Kroll.

What You Can Do. You can learn more about the complimentary consultation services through Kroll and find out more about how to help protect against potential identity theft and fraud in the enclosed Steps You Can Take to Help Protect Your Loved One's Information. Your loved one's Membership Number is <<Member ID>>.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-???-???-????, Monday through Friday (except U.S. holidays), during the hours of 8:00 a.m. to 5:30 p.m., Central Time. You may also write to University of Minnesota Physicians at 720 Washington Avenue SE Suite #200, Minneapolis, MN 55414; Attention: Compliance Officer.

We are very sorry this incident occurred and sincerely regret any inconvenience or concern it may

cause.

Sincerely,

Sara DeSanto
Compliance Officer
University of Minnesota Physicians

STEPS YOU CAN TAKE TO HELP PROTECT YOUR LOVED ONE'S INFORMATION

Monitor Your Accounts

We recommend obtaining a copy of your loved one's credit report to review whether there are any active credit accounts that need to be closed or any pending collection notices that need to be addressed. If you have not already done so, you may also request, in writing, that your loved one's credit report is flagged with the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

A spouse or executor of the estate may request a copy of your loved one's credit report or flag your loved one's credit report with the above alert. This must be requested in writing and should include the below information:

Information related to your loved one:

- Legal name
- Social Security Number
- Date of Birth
- Date of Death
- Last Known address
- A copy of the death certificate or letters testamentary. A letters testamentary is a document issued by a court or public official authorizing the executor of a will to take control of a deceased person's estate.

Information related to the individual requesting the information or placing the alert:

- Full name
- Address for sending final confirmation
- In the case of an executor, include the court order or other document indicating the executor of the estate

In most cases, a flag will prevent the opening of new credit accounts in your loved one's name. Mailing and contact information for the three major credit bureaus is as follows:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

If you find suspicious activity on your credit reports or have reason to believe your information has been misused, the Federal Trade Commission encourages you to file a report with its Fraud Department. Your report will be added to the FTC's Identity Theft Data Clearinghouse. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. You also have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

For Maryland residents: The Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; and www.oag.state.md.us.

For North Carolina residents: The Attorney General may be contacted at 9001 Mail Service Center, Raleigh; NC 27699-9001, 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information;

consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents: The Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [x] Rhode Island residents impacted by this incident.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and https://ag.ny.gov/.

For Washington, D.C. residents: The Attorney General may be contacted at: Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001; (202) 727-3400; and www.oag@dc.gov.

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF FRAUD CONSULTATION AND IDENTITY THEFT RESTORATION SERVICES

You have been provided with access to the following services from Kroll:

Fraud Consultation . You have unlimited access to consultation with a Kroll fraud specialist. Support includes interpreting how personal information is accessed and used, explaining your rights and protections under the law, assistance with fraud alerts, and showing you the most effective ways to protect personal information, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration . An experienced Kroll licensed investigator will work on your behalf to resolve issues related to identity theft. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator will be able to dig deep to uncover all aspects of the identity theft, and then work to resolve it.

EXHIBIT B

UMP - HIPAA Website Notice – Phase Two

November 25, 2020 – University of Minnesota Physicians ("UMPhysicians") is issuing notice of a data security event that potentially affected the confidentiality of personal information of certain patients.

What Happened. UMPhysicians recently completed a thorough investigation and comprehensive data review of a data security event in which cyber attackers used phishing emails to fraudulently access two employee email accounts. The two phishing email attacks were identified on January 31, 2020 and February 4, 2020, shortly after they occurred. UMPhysicians took immediate steps to secure the email accounts and began working with third-party computer forensic investigators to determine the nature and scope of the incidents. The investigation indicated that an unknown actor had access to one employee email account on January 30 and January 31, 2020, and another employee email account on February 4, 2020, for a brief period of time.

Unfortunately, the investigation was unable to determine with certainty to what extent any emails within the two accounts may have been viewed by the cyber attackers. Based on this, in an abundance of caution, we retained third-party specialists to perform a comprehensive review of all information stored in the email accounts at the time of the incidents to identify any personal information present in the accounts. The employee email accounts contained information about individuals because the email accounts were used to perform normal business operations related to health care services provided by UMPhysicians. On March 30, 2020, UMPhysicians began notifying individuals with information present in the accounts while its review was ongoing. Upon completion of the third-party specialists' review of the full contents of the email accounts, which was a detailed and lengthy process that involved multiple steps to identify the relevant data, we immediately began assessing the results to confirm the identities of potentially affected individuals and obtain their current mailing addresses or other contact information. We recently completed this comprehensive review process.

What Information was Affected. The review determined that one or more of the following types of information associated with an individual were present in an affected email account during the incident: name, address, date of birth, date of death, date of service, telephone number, medical record number, account number, payment card number, health insurance information, and medical information. For a small number of individuals, it may also include Social Security number. We have no evidence indicating that this information was actually viewed during the incident or has been copied or otherwise misused. However, the perpetrators did have access to the two email accounts for a limited period of time so it is possible they may have seen some information.

What We Are Doing. UMPhysicians takes this incident and the security of the information in its care very seriously. We quickly identified the attacks and took steps to secure the affected email accounts. At the time of the attacks, UMPhysicians had multiple email security controls in place, including multi-factor authentication. We also require all employees to participate in privacy and security training, and we regularly conduct exercises to try to make sure personnel do not fall prey to phishing and related scams. As part of our ongoing commitment to the privacy and security of personal information in our care, we reviewed our policies and procedures and implemented additional safeguards to further control and secure the information in our email system. For example, we conducted refresher training for personnel related to best practices in identifying phishing attempts, and we implemented restrictions on email retention. We also purchased additional technology that will provide for more enhanced detection and prevention of phishing emails. In addition, we notified state and federal regulators where we are required to do so.

What Affected Individuals Can Do. While we are unaware of any misuse of any personal information contained within the impacted email accounts, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and reporting

any suspicious activity immediately to their insurance company, health care provider, or financial institution. In addition, we are offering affected individuals access to complimentary identity and credit monitoring services for 12 months through Kroll. Additional detail can be found below, in the *Steps You Can Take to Protect Your Personal Information.*

For More Information. Individuals seeking additional information regarding this event can call our toll-free assistance line at (833) 960-3571, Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 5:30 p.m., Central Time. You may also write to University of Minnesota Physicians at 720 Washington Avenue SE #200, Minneapolis, MN 55414.

Steps You Can Take To Protect Your Personal Information

While we are unaware of any misuse of the personal information in the impacted email account, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

If you wish to enroll with the Kroll credit monitoring and identity restoration services, please contact our dedicated assistance line to verify that your information was contained within the two email accounts. After confirmation that you were included, Kroll will assist in enrolling you in the credit monitoring service.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior

five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

EXHIBIT C

University of Minnesota Physicians Provides Notice of Data Security Event

Minneapolis, Minnesota November 25, 2020 – Today, University of Minnesota Physicians ("UMPhysicians") issued notice of a data security event that potentially affected the confidentiality of personal information related to certain patients.

UMPhysicians recently completed a thorough investigation and comprehensive data review of a data security event in which cyber attackers used phishing emails to fraudulently access two employee email accounts. The two phishing email attacks were identified on January 31, 2020 and February 4, 2020, shortly after they occurred. UMPhysicians took immediate steps to secure the email accounts and began working with third-party computer forensic investigators to determine the nature and scope of the incidents. The investigation indicated that an unknown actor had access to one employee email account on January 30 and January 31, 2020, and another employee email account on February 4, 2020, for a brief period of time.

Because the investigation was unable to determine with certainty to what extent any emails within the two accounts may have been viewed by the cyber attackers, in an abundance of caution, UMPhysicians retained third-party specialists to perform a comprehensive review of all information stored in the email accounts at the time of the incident to identify any personal information present in the accounts. On March 30, 2020, UMPhysicians began notifying individuals with information present in the accounts while its review was ongoing. UMPhysicians recently completed the comprehensive data review, which involved many detailed steps to identify and confirm the relevant data and the potentially affected individuals. UMPhysicians is now notifying the additional individuals who were identified as potentially affected

The recently completed data review identified that one or more of the following types of information associated with an individual were present in an affected email account during the incident: name, address, date of birth, date of death, date of service, telephone number, medical record number, account number, payment card number, health insurance information, and medical information. For a small number of individuals, it may also include Social Security number. There is no evidence indicating that this information was actually viewed during the incident or has been copied or otherwise misused.

UMPhysicians is notifying potentially affected individuals by this posting, notification on its website, and by mailing letters to potentially affected individuals. For individuals seeking additional information regarding this incident, a dedicated toll-free assistance line has been established. Individuals may call the assistance line at (833) 960-3571, Monday through Friday (excluding U.S. holidays), during the hours of 8 a.m. to 5:30 p.m., Central Time.

Individuals can also find additional information on how they can protect their personal information as well as obtain additional resources on UMPhysicians' website https://mphysicians.org/ and in the letters they will receive by mail. UMPhysicians is offering individuals complimentary identity and credit monitoring for one year. As a precautionary measure, UMPhysicians encourages potentially affected individuals to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and reporting any suspicious activity immediately to their insurance company, health care provider, or financial institution.

UMPhysicians takes this incident and the security of the information in its care very seriously. As part of UMPhysicians' ongoing commitment to its patients, UMPhysicians has implemented a range of privacy and security safeguards designed to enhance the protections it has in place against phishing and similar malicious attacks, including the deployment of additional security technology and security awareness training. UMPhysicians deeply regrets that this matter occurred and sincerely apologizes for any inconvenience or concern it may have caused.

# # #