POLSINELLI

1401 Eye Street NW, Suite 800, Washington, DC 20005 • (202) 783-3300

July 2, 2019

Iliana L. Peters
(202) 626-8327
(202) 403-3902 Direct Fax
ipeters@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of a Data Security Incident - Update

Dear Attorney General MacDonald:

We represent Navicent Health in connection with a recent incident that may have impacted the personal information of twenty-three (23) New Hampshire residents, and provide this notice on behalf of Navicent Health pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice supplements our previous notice dated March 22, 2019, due to our discovery of a significant error committed by a vendor, Epiq, that had impacted Navicent's understanding of the number of individuals potentially impacted by the incident subsequent to the notice submission. While Navicent Health is notifying you of this supplementary information pertaining to the incident, Navicent Health does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

Navicent Health was the victim of a cyber attack in July, in which an unauthorized third party illegally accessed employee email accounts. Upon learning of the attack, Navicent Health commenced a prompt, extensive, and thorough investigation. As part of Navicent Health's investigation, Navicent Health worked closely with four industry-leading, external data privacy and cybersecurity firms experienced in handling these types of issues. After a broad forensic investigation, Navicent Health discovered on January 24, 2019, that the impacted email accounts that were accessed contained personal information for certain individuals.

At this point, Navicent Health is not aware of any fraud or identity theft to any individual as a result of this incident, and does not know if any personal information was ever viewed or acquired by the unauthorized party. It is also important to note that the incident impacted

employee email accounts only, and had no impact on Navicent Health's computer networks or electronic medical record systems. However, Navicent Health has notified potentially impacted patients and has provided information on steps they can take to protect themselves against fraud or identity theft.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Navicent Health immediately took action, including deleting impacted account credentials to prevent further access and confirming the security of our email system. Navicent Health also notified law enforcement and retained leading forensic security firms to investigate and conduct a comprehensive search for any personal information on the impacted email accounts. It is important to note that the incident had no impact on Navicent Health's computer networks or electronic medical record systems. Navicent Health also provided complimentary identity theft protection services to all individuals whose social security numbers were contained in the email account through Experian.

NEWLY DISCOVERED INFORMATION PERTAINING TO THE INCIDENT

On April 17, 2019, Epiq notified Navicent that it made a mistake that resulted in Epiq wrongly associating a large group of individuals with a different entity related to this incident instead of Navicent Health that affected Navicent Health's notification of the breach incident. Epiq was responsible for manually reviewing approximately 23,000 emails and attachments to provide Navicent Health with a list of individuals whose personal information was found in the email accounts, as well as information regarding the type of personal information found in the account for each person, in general terms. On May 3, 2019, Epiq verified their mistake. The additional individuals for whom Navicent Health is sending notification in New Hampshire are part of the misidentified group of individuals by Epiq.

STEPS TAKEN RELATING TO THE NEWLY DISCOVERED INFORMATION PERTAINING TO THE INCIDENT

Upon learning of Epiq's error, Navicent Health again immediately took action, including working to obtain addresses for the additional individuals and to de-duplicate any individuals, including those to whom Navicent Health has already provided notification. Navicent Health is providing notification to the newly identified individuals and offering complimentary identity theft protection services to all of those individuals whose social security numbers were contained in the email account through Experian for 12 months.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Based on the previously discovered information, Navicent Health mailed notification letters to

POLSINELLI

twenty (20) New Hampshire residents who may have been impacted by the incident starting on March 21, 2019.

Based on the newly discovered information, an additional three (3) New Hampshire residents may have been impacted. Enclosed is a copy of the notices that Navicent Health has sent to those individuals starting on June 18, 2019.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Iliana L. Peters

Enclosures

NavicentHealth
Everything about us is all about you.

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<LastName>>,

We value and respect the privacy of your information, which is why we are writing to advise you of a cyber-attack that occurred this past summer that may have involved some of your personal information. As a result of our investigation of the attack, we recently learned that some of your information could have been viewed by an unauthorized third-party that illegally accessed Navicent Health employee email accounts.

Upon learning of the incident in July, we promptly instigated a security incident investigation. We also notified law enforcement and retained leading forensic security firms to help us investigate and conduct a comprehensive search for any personal information in the impacted email accounts, and to confirm the security of our email and computer systems. On January 24, 2019, our investigation determined that the email accounts that may have been accessed contained some personal information. The information for each affected individual differs but may have included your name, date of birth, bank account and/or medical information – for example, information such as medical record numbers, dates of service, physician seen, a brief summary of medical condition and services provided, and billing information. The incident did not impact your Social Security Number.

It is important to know that at this point, we do not know for certain if any personal information was ever viewed by the unauthorized party, and are not aware of any instances of fraud or identity theft as a result of this incident. However, out of an abundance of caution we are notifying you of the incident nonetheless.

We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. We are committed to taking steps to help prevent something like this from happening again, including evaluating additional platforms for educating staff and reviewing technical controls. For further information and assistance, please call 1-866-681-5170 from 9:00 a.m. to 6:30 p.m. ET, Monday through Friday.

Sincerely,

Roy Griffis, Jr.
Navicent Health Privacy Officer

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting http://www.annualcreditreport.com, by calling toll free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit bureau. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies using the contact information above.

In order to request a security freeze, you may 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;

The credit bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To remove the security freeze or lift the freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit bureaus have three (3) business days after receiving your request to remove or lift the security freeze for those identified entities or for the specified period of time.

If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Georgia Attorney General's Office at 800-436-7433.

Individuals interacting with credit bureaus have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 220 St. Paul Place, Baltimore, MD 21202, (888) 743-0023.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226.

Rhode Island Residents: We believe that this incident affected ### Rhode Island residents.. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400.

NavicentHealth
Everything about us is all about you.

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

Parent or Guardian of
<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear Parent or Guardian of <<FirstName>> <<LastName>>,

We value and respect the privacy of your child's information, which is why we are writing to advise you of a cyber-attack that occurred this past summer that may have involved some of your child's personal information. As a result of our investigation of the attack, we recently learned that some of your child's information could have been viewed by an unauthorized third-party that illegally accessed Navicent Health employee email accounts.

Upon learning of the incident in July, we promptly instigated a security incident investigation. We also notified law enforcement and retained leading forensic security firms to help us investigate and conduct a comprehensive search for any personal information in the impacted email accounts, and to confirm the security of our email and computer systems. On January 24, 2019, our investigation determined that the email accounts that may have been accessed contained some personal information. The information for each affected individual differs but may have included your child's name, date of birth, bank account and/or medical information – for example, information such as medical record numbers, dates of service, physician seen, a brief summary of medical condition and services provided, and billing information. The incident did not impact your child's Social Security Number.

It is important to know that at this point, we do not know for certain if any personal information was ever viewed by the unauthorized party, and are not aware of any instances of fraud or identity theft as a result of this incident. However, out of an abundance of caution we are notifying you of the incident nonetheless.

We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. We are committed to taking steps to help prevent something like this from happening again, including evaluating additional platforms for educating staff and reviewing technical controls. For further information and assistance, please call 1-866-681-5170 from 9:00 a.m. to 6:30 p.m. ET, Monday through Friday.

Sincerely,

Roy Griffis, Jr.
Navicent Health Privacy Officer

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your child's account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your child's credit report, if one exists, once every 12 months from each of the three national credit reporting agencies by visiting http://www.annualcreditreport.com, by calling toll free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf.

Alternatively, you may elect to purchase a copy of your child's credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your child's credit report. An initial fraud alert is free and will stay on your child's credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your child's name. To place a fraud alert on your child's credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your child's credit file, so that no new credit can be opened in your child's name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your child's credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your child's credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your child's ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your child's credit file at each credit bureau. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies using the contact information above.

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

1. Your child's 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;

The credit bureaus have three (3) business days after receiving your request to place a security freeze on your child's credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To remove the security freeze or lift the freeze in order to allow a specific entity or individual access to your child's credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your child's credit report or the specific period of time you want the credit report available. The credit bureaus have three (3) business days after receiving your request to remove or lift the security freeze for those identified entities or for the specified period of time.

If you do not have internet access but would like to learn more about how to place a security freeze on your child's credit report, contact the Georgia Attorney General's Office at 800-436-7433.

Individuals interacting with credit bureaus have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 220 St. Paul Place, Baltimore, MD 21202, (888) 743-0023.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226.

Rhode Island Residents: We believe that this incident affected ### Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400.