MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

November 23, 2020

VIA FIRST-CLASS MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Premier Health Partners ("Premier Health") located at 101 N. Main Street, Suite 930, Dayton, Ohio 45402, and write to notify your office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Premier Health does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 8, 2020, Premier Health discovered unusual activity involving certain Premier Health employee email accounts. Premier Health immediately reset passwords to the accounts and commenced an investigation that included working with computer forensic specialists to understand the full scope of accounts impacted. On July 17, 2020, Premier Health confirmed certain accounts were subject to unauthorized access by someone not connected with Premier Health beginning on May 5, 2020. The investigation confirmed access to the accounts occurred on separate occasions between May 5 and June 16, 2020. Because the investigation could not conclusively rule out access to data within the accounts, Premier Health commenced a full review of the contents of the accounts to determine all records that were present.

Premier Health received initial results of the account review on August 18, 2020, while the investigation continued. On October 12, 2020, Premier Health received the full results of the

review of all information in the impacted email accounts. Premier Health then worked diligently to identify last known address information for those individuals identified as impacted in the final review. On November 6, 2020, Premier Health confirmed address information for a certain population of individuals with sensitive information present in the compromised accounts. The information that could have been subject to unauthorized access includes name and/or Social Security number.

Notice to New Hampshire Residents

Premier Health began providing notification to impacted individuals between August 7, 2020 and October 2, 2020. As a result of the continued investigation and data review, on or about November 20, 2020, Premier Health will provide written notice of this incident to additional individuals, including approximately two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. On August 7, 2020, Premier Health also posted notice of this incident to its website and provided notice to statewide media in Ohio.

Other Steps Taken and To Be Taken

Upon discovering the event, Premier Health moved quickly to investigate and respond to the incident, assess the security of Premier Health systems, and notify potentially affected individuals. Premier Health is retraining staff and implementing additional safeguards to further secure the information in its systems. Premier Health is also providing access to credit monitoring services for twelve (12) months, from CyberScout (through Epiq), to individuals whose Social Security number or driver's license/state identification number was potentially affected by this incident, at no cost to these individuals.

Additionally, Premier Health is providing all individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Premier Health is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Premier Health notified law enforcement, its relevant federal regulator, and other state regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,

M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/nsj

EXHIBIT A

Premier Health

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

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

<<Date>>

Re: Data Privacy Incident

Dear <<Name1>>:

Premier Health Partners ("Premier Health") writes to make you aware of a recent incident that may affect the privacy of personal information for certain individuals associated with the Clinical Neuroscience Institute, Help Me Grow Brighter Futures, Samaritan Behavior Health Inc. (SBHI), Atrium Medical Center, Miami Valley Hospital, Miami Valley Hospital North, and CompuNet Clinical Laboratories. While we have no evidence of any actual or attempted misuse of information at this time, we are providing you with information about the event, the steps we have taken and are taking in response, and additional precautions you can take, should you feel it is appropriate to do so.

What Happened? On June 8, 2020, Premier Health discovered unusual activity involving certain Premier Health employee email accounts. We immediately reset passwords to the accounts and commenced an investigation that included working with computer forensic specialists to understand the full scope of accounts impacted. On July 17, 2020, we confirmed certain accounts were subject to unauthorized access by someone not connected with Premier Health beginning on May 5, 2020. The investigation confirmed access to the accounts occurred on separate occasions between May 5 and June 16, 2020. Because the investigation could not conclusively rule out access to data within the accounts, we commenced a full review of the contents of the accounts to determine all records that were present. While our investigation is ongoing, we received results of the account review on October 12, 2020. Since that time, Premier Health has been working diligently to identify and determine contact information for those individuals whose information was identified. On November 6, 2020, Premier Health confirmed address information for a certain population of the individuals with sensitive information present in the compromised accounts and immediately began taking steps to provide those individuals with notice of this incident.

What Information Was Involved? While we currently have no evidence that any information was subject to actual or attempted misuse, the investigation confirmed that your contact information, <<Data Elements>> were present in the affected accounts at the time of the incident.

What We Are Doing. Premier Health takes the privacy and security of information in our care very seriously. Since discovering this event, we have been working diligently with computer forensic specialists to determine what happened and what data was potentially impacted. We are retraining staff and implementing additional safeguards to further secure the information in our systems. Although we have no indication that information was or will be misused, we are providing potentially impacted individuals notice of this event, as well as information and resources to assist you in protecting your personal information, should you feel it appropriate to do so.

Premier Health has also secured the services of CyberScout to provide you with access to credit monitoring and identity restoration services for twelve (12) months, at no cost to you. More information on these services can be found in the enclosed "Steps You Can Take to Protect Your Information."

What You Can Do. Premier Health encourages you to remain vigilant against incidents of fraud or identity theft, and to monitor your accounts, explanation of benefits, and free credit reports for suspicious activity and to detect errors. Please also review the resources we are providing in the attached "Steps You Can Take to Protect Your Information."

For More Information. If you have questions that are not addressed in this letter, please call our dedicated assistance line at 888-905-0023, available Monday through Friday, from 9:00 a.m. to 9:00 p.m., Eastern Time.

We sincerely regret any inconvenience or concern this event may cause you. Please know we take this incident seriously and are committed to the privacy and security of information in our care.

Respectfully,

Steven R. Walker

Steven R. Walker
Director, Information Security and Privacy

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

We are providing you with access to Single Bureau Credit Monitoring services at no charge. Services are for one year from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to https://www.myidmanager.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Activation Code>>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Monitor Accounts

Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) 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 30348-5788
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

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.); and
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 one (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 19106	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-alerts	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. 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. 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. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us. 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 violators. 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 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 Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 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 2 Rhode Island residents impacted by this incident.

For District of Columbia residents, the District of Columbia Attorney General can be reached at 441 4th St. NW #1100 Washington, D.C. 20001, by phone at (202) 727-3400 and by email at oag@dc.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.