Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 14, 2020

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. 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 Aveanna Healthcare ("Aveanna"), 400 Interstate North Parkway SE, Suite 1600, Atlanta, GA 30339. We write to notify you of a recent incident that may affect the security of the personal information of sixty-two (62) New Hampshire residents. By providing this notice, Aveanna does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

Beginning on August 24, 2019, Aveanna became aware of suspicious activity relating to a number of its employee email accounts. Aveanna took steps to secure the email accounts and began working with outside computer forensics specialists to determine the nature and scope of the activity. The investigation determined that an unknown actor accessed certain employee email accounts between July 9, 2019 and August 24, 2019. Unfortunately, the investigation did not reveal if any email or attachment was actually accessed or viewed.

In an abundance of caution and with the assistance of third-party specialists, a comprehensive review of the contents of the impacted email accounts was performed to identify any personal information that could have potentially been viewed or acquired by the intruder. Once this exhaustive review was complete, we next worked diligently to confirm the identity of the impacted individuals to whom that information related and their address. The investigation recently concluded, and Aveanna is providing notice to individuals whose personal information may have been accessible.

Although the type of personal information potentially impacted may vary by individuals, Aveanna confirmed that the following types of personal information relating to sixty-two (62) New Hampshire residents were present within impacted email accounts: Social Security number and bank or financial account number.

Notice to New Hampshire Residents

Aveanna began mailing written notice to potentially affected individuals, which includes sixty-two (62) New Hampshire residents, on or about February 14, 2020. Notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and to Be Taken

Upon discovering the incident, Aveanna moved quickly to determine its nature and scope. Aveanna identified the individuals who may be affected by the incident, put resources in place to assist them, and provided them with notice.

Aveanna is providing all potentially affected individuals with complimentary access to twelve (12) months of credit monitoring and identity restoration services through TransUnion. Additionally, Aveanna is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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 identity theft and fraud 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.

While Aveanna had security measures in place to protect information in its care, it also took steps to implement additional safeguards and review company policies and procedures in order to ensure it protects the security of information on its systems. Specifically, Aveanna immediately changed the credentials for the involved email accounts and has since implemented additional security measures for employee email accounts and access to company systems including multi-factor authentication.

Aveanna is providing notice of this incident to other state and federal regulators and the three major credit reporting agencies, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

Enclosure
RCL/ras

EXHIBIT A

aveanna
healthcare

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>>

Dear <<Name 1>>:

Aveanna Healthcare ("Aveanna" or the "Company") is writing to inform you of an incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can better protect against the possibility of misuse of your personal information, should you feel it appropriate to do so.

What Happened? Beginning on August 24, 2019, Aveanna became aware of suspicious activity relating to a number of its employee email accounts. Aveanna took steps to secure the email accounts and began working with outside computer forensics specialists to determine the nature and scope of the activity. The investigation determined that an unknown actor accessed certain employee email accounts between July 9, 2019 and August 24, 2019. Unfortunately, the investigation did not reveal if any email or attachment was actually accessed or viewed.

In an abundance of caution and with the assistance of third-party specialists, a comprehensive review of the contents of the impacted email accounts was performed to identify any personal information that could have potentially been viewed or acquired by the intruder. Once this exhaustive review was complete, we next worked diligently to confirm the identity of the impacted individuals to whom that information related and their address. On December 19, 2019, we determined that information for certain patients and Company employees may have been accessible within the email accounts involved in this event.

What Information Was Involved? The investigation determined the following types of your personal information were present in at least one of the impacted email accounts at the time it was subject to unauthorized access: your <<Data Elements2-Impacted Info>> and name. **Please note our investigation was not able to determine whether your information was actually viewed or taken by the unauthorized intruder, and we are not currently aware of any actual or attempted misuse of any personal or protected health information in relation to this incident.**

What We Are Doing. Aveanna takes the confidentiality, privacy, and security of information in its care very seriously. While Aveanna has security measures in place to protect information in its care, we are also taking steps to implement additional safeguards and review Company policies and procedures in order to ensure we protect the security of information on our systems. Specifically, Aveanna immediately changed the credentials for the involved email accounts and has since implemented additional security measures for employee email accounts and access to Company systems including multifactor authentication.

As an added precaution, Aveanna is providing you with access to <<Data Elements1-Monitoring Length>> months of credit monitoring and identity protection services from TransUnion at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information*. You can also enroll to receive the free credit monitoring services and identity protection services through TransUnion.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions or concerns, please call our dedicated hotline at 866-977-0742, Monday through Friday, 9 am to 9 pm Eastern Time, excluding national holidays.

Please know Aveanna takes the privacy and security of the personal information in our care very seriously, and we sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Patrick Cunningham
Chief Compliance Officer
Aveanna Healthcare

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

Complimentary <<Data Elements1-Monitoring Length>> **Month *my*TrueIdentity Credit Monitoring Service**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<Data Elements1-Monitoring Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR <<Data Elements1-Monitoring Length>> MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<Data Elements1-Monitoring Length>> months of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Your Accounts

In addition to enrolling in the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. 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	PO Box 105788
Allen TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	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 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-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.

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. This notice has not been delayed by law enforcement.

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.

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 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 74 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; https://ag.ny.gov/.

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.