McDonald Hopkins
A business advisory and advocacy law firm®

LANE POWELL

SIGNATURE healthcare at home
care where you are

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Lane Powell PC
601 SW Second Avenue, Suite 2100
Portland, OR 97204-3158

November 28, 2022

VIA U.S. MAIL

Office of Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104

Re: Avamere Health Services, LLC – Incident Notification (Final Update)

To Whom It May Concern:

As discussed in prior correspondence, the undersigned counsel jointly represent Avamere Health Services, LLC and affiliated employers ("Avamere"), Signature Healthcare at Home affiliated employers ("Signature"), and Premere Rehab, LLC ("Infinity Rehab"). We are writing to provide a further update to our letters to your office dated June 17, 2022, July 13, 2022, and August 10, 2022 (hereinafter, our "Preliminary Notifications").

As discussed in our Preliminary Notifications, Avamere Health Services, LLC provides certain information technology services to Infinity Rehab, Signature, and other affiliated entities. Avamere, Signature, and Infinity Rehab are collectively referenced herein as "the Entities." By providing this final update to our Preliminary Notifications, the Entities do not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction. This letter will be supplemented with any new or significant facts or findings subsequent to this submission, if any.

As discussed in our Preliminary Notifications, the Entities determined that intermittent unauthorized access to a third-party hosted network utilized by Avamere Health Services, LLC occurred between January 19, 2022 and March 17, 2022 (hereinafter, the "Incident"). Our Preliminary notifications also represented that, upon learning of the issue, the Entities promptly opened an investigation. As part of the investigation, the Entities have been working closely with external cybersecurity professionals. The Entities' investigation of the Incident, which entailed both data mining and an extensive manual document review exercise, concluded on or about October 18, 2022.

As discussed in our Preliminary Notifications, the Entities determined that an unauthorized party potentially acquired a limited number of electronic files and folders belonging to the Entities that contain personal information of certain individuals. As an update to our Preliminary Notifications, Avamere and Infinity Rehab have concluded that the known

approximate total population of Washington residents impacted by the Incident is sixty-five thousand and seventy-six (65,076).

The Entities are providing those individuals that have not yet received notification letters with written notification of this incident commencing on or about November 22, 2022 in substantially the same form as the letter attached hereto as **Exhibit A**. All notified individuals will be provided complimentary credit monitoring services with the notification letter. The Entities are advising the individuals about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. Further, the individuals are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority for the Entities. The Entities are committed to maintaining the privacy of personal information in their possession and have taken many precautions to safeguard it. The Entities continually evaluate and modify their practices and internal controls to enhance the security and privacy of personal information. The Entities have implemented enhanced security safeguards to help protect against similar intrusions from occurring in the future.

Should you have any questions regarding this notification, please contact Dominic Paluzzi at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Dominic A. Paluzzi	Barbara J. Duffy	Carrie Vanderzanden
McDonald Hopkins PLC	Lane Powell PC	Signature Healthcare at Home

Encl.

To Enroll, Please Call:
[redacted]
Or Visit:
[redacted]
Enrollment Code:
[redacted]

Avamere Health Services
[redacted]

[redacted]

[redacted]

Dear [redacted]:

We, Avamere Health Services, LLC provide information technology services to health care providers. We are writing to inform you of a data security incident involving some of your information in connection with [redacted] We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

We recently determined that intermittent unauthorized access to our network occurred between January 19, 2022 and March 17, 2022.

What We Are Doing.

Upon learning of this issue, we immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to assess the extent of any compromise. After an extensive investigation, we concluded on October 18, 2022 that an unauthorized party potentially removed a limited number of files and folders from our system that may contain your personal information.

What Information Was Involved?

The acquired files potentially contained your [redacted].

What You Can Do.

We want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary [redacted]-year membership of identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: [redacted] months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on your complimentary [redacted]-year membership, please see the additional information provided in this letter.

[redacted]

This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

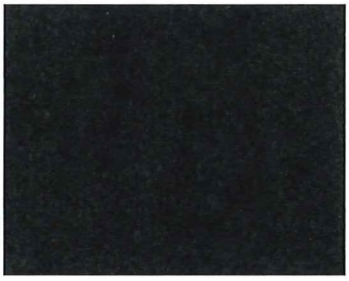
For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 6 am to 6 pm Pacific Time.

Sincerely,

Avamere Health Services, LLC



– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [redacted] Month Credit Monitoring.

Activate IDX Identity Protection Membership Now in Three Easy Steps

1. ENROLL by: February 18, 2023 (Your code will not work after this date.)
2. VISIT the IDX website to enroll: [redacted]
3. PROVIDE the Enrollment Code: [redacted]

If you have questions about the product or if you would like to enroll over the phone, please contact IDX at 833-909-4422.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary [redacted]-month credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

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

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

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

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

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

McDonald Hopkins
A business advisory and advocacy law firm®
LANE POWELL

SIGNATURE healthcare at home
care where you are

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Lane Powell PC
601 SW Second Avenue, Suite 2100
Portland, OR 97204-3158

VIA U.S. MAIL

Bob Ferguson
Office of Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104

Re: Avamere Health Services, LLC – Incident Notification

Dear Mr. Ferguson:

The undersigned counsel jointly represent Avamere Health Services, LLC and affiliated employers ("Avamere"), Signature Healthcare at Home and affiliated employers ("Signature"), and Premere Rehab, LLC ("Infinity Rehab"). Avamere Health Services, LLC provides certain information technology services to Infinity Rehab, Signature, and other affiliated entities. Avamere, Infinity Rehab, and Signature are collectively referenced herein as "the Entities."

We are writing to provide notification of an incident that may affect the security of personal information of approximately eleven thousand three hundred and eighty-three (11,383) Washington residents (hereinafter, the "Employees") who are or have been employed by one or more of the Entities. By providing this notice, the Entities do not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction. The Entities' investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any.

The Entities recently determined that intermittent unauthorized access to a third-party hosted network utilized by Avamere Health Services, LLC occurred between January 19, 2022 and March 17, 2022. Upon learning of the issue, the Entities promptly opened an investigation. As part of the investigation, the Entities have been working closely with external cybersecurity professionals.

After an extensive forensic investigation, the Entities concluded on May 18, 2022 that an unauthorized party potentially acquired a limited number of electronic files and folders belonging to the Entities that contain personal information of the Employees. Specifically, the information that potentially may have been acquired included the Employees' full names, dates

of birth, Social Security numbers, and medical information. Impacted elements of information varied per individual.

To date, the Entities are not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, the Entities wanted to inform you (and the affected Employees) of the incident and to explain the steps that the Entities are taking to help safeguard the Employees against identity fraud.

The Entities are providing the Employees with written notification of this incident commencing on or about June 17, 2021 in substantially the same form as the letter attached hereto. All Employees will be provided complimentary credit monitoring services with the notification letter. The Entities are advising the Employees about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. Further, the Employees are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority for the Entities. The Entities are committed to maintaining the privacy of personal information in their possession and have taken many precautions to safeguard it. The Entities continually evaluate and modify their practices and internal controls to enhance the security and privacy of personal information. The Entities have implemented enhanced security safeguards to help protect against similar intrusions from occurring in the future.

Should you have any questions regarding this notification, please contact Dominic Paluzzi at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Dominic A. Paluzzi	Barbara J. Duffy	Carrie Vanderzanden
McDonald Hopkins PLC	Lane Powell PC	Signature Healthcare at Home

Encl.

EXHIBIT A

To Enroll, Please Call:
[redacted]
Or Visit:
[redacted]
Enrollment Code:
[redacted]

P.O. Box 1907
Suwanee, GA 30024

[redacted]

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear [redacted]:

We are writing to inform you of a data security incident involving some of your information in connection with your employment at [redacted]. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

We recently determined that intermittent unauthorized access to a network controlled by Avamere Health Services, LLC occurred between January 19, 2022 and March 17, 2022. Avamere Health Services, LLC provides certain information technology services to the employer(s) listed above.

What We Are Doing.

Upon learning of this issue, we immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to assess the extent of any compromise. After an extensive investigation, we concluded on May 18, 2022 that an unauthorized party potentially removed a limited number of files and folders from our system that may contain your personal information.

What Information Was Involved?

The acquired files potentially contained your [redacted].

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary [redacted]-year membership of identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: [redacted] months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on your complimentary [redacted]-year membership, please see the additional information provided in this letter.

This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and entrusted to others and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 6 am to 6 pm Pacific Time.

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [redacted]-Months Credit Monitoring.

Activate IDX Identity Protection Membership Now in Three Easy Steps

1. ENROLL by: October 13, 2022 (Your code will not work after this date.)
2. VISIT the IDX website to enroll: https://response.idx.us/avamere
3. PROVIDE the Enrollment Code: [redacted]

If you have questions about the product or if you would like to enroll over the phone, please contact IDX at 833-909-4422.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary [redacted]-months credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

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

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

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

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

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

McDonald Hopkins
A business advisory and advocacy law firm®
LANE POWELL

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Lane Powell PC
601 SW Second Avenue, Suite 2100
Portland, OR 97204-3158

July 13, 2022

VIA U.S. MAIL

Bob Ferguson
Office of Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104

Re: Avamere Health Services, LLC – Incident Notification (Update)

To Whom It May Concern:

The undersigned counsel jointly represent Avamere Health Services, LLC and affiliated entities ("Avamere"), and Premere Rehab, LLC ("Infinity Rehab"). We are writing to provide an update to our letter to your office dated June 17, 2022 (hereinafter, our "Preliminary Notification"). As discussed in our Preliminary Notification, Avamere Health Services, LLC provides certain information technology services to Infinity Rehab and other affiliated entities as a Business Associate as defined at 45 CFR § 160.103. Avamere and Infinity Rehab are collectively referenced herein as "the Entities."

By providing this update to our Preliminary Notification, the Entities do not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction. The Entities' investigation remains ongoing, and this letter will be supplemented with any new or significant facts or findings subsequent to this submission, if any.

As discussed in our Preliminary Notification, the Entities recently determined that intermittent unauthorized access to a third-party hosted network utilized by Avamere Health Services, LLC occurred between January 19, 2022 and March 17, 2022. Our Preliminary Notification also represented that, upon learning of the issue, the Entities promptly opened an investigation. As part of the investigation, the Entities have been working closely with external cybersecurity professionals.

Additionally, as discussed in our Preliminary Notification, the Entities concluded on May 18, 2022 that an unauthorized party potentially acquired a limited number of electronic files and folders belonging to the Entities that contain personal information of certain individuals.

As an update to our Preliminary Notification, the investigation has determined that approximately thirty one thousand six hundred and ninety-five (31,695) additional Washington residents (hereinafter, the "Patients") were impacted by the Incident. Specifically, the information that potentially may have been acquired with respect to the Patients included the Patients' full names, addresses, dates of birth, driver's license or state identification numbers,

Social Security numbers, claims information, financial account numbers, medications information, lab results, and medical diagnosis/conditions information. Impacted elements of information varied per individual.

The Entities are providing the Patients with written notification of this incident commencing on or about July 13, 2022 in substantially the same form as the letter attached hereto as Exhibit A. All Patients will be provided complimentary credit monitoring services with the notification letter. The Entities are advising the Patients about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. Further, the Patients are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority for the Entities. The Entities are committed to maintaining the privacy of personal information in their possession and have taken many precautions to safeguard it. The Entities continually evaluate and modify their practices and internal controls to enhance the security and privacy of personal information. The Entities have implemented enhanced security safeguards to help protect against similar intrusions from occurring in the future.

Should you have any questions regarding this notification, please contact Dominic Paluzzi at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Dominic A. Paluzzi
McDonald Hopkins PLC

Barbara J. Duffy
Lane Powell PC

Encl.

EXHIBIT A

Avamere Health Services
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
[redacted]
Or Visit:
https://response.idx.us/avamere
Enrollment Code: [redacted]

[redacted]

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear [redacted]:

We, Avamere Health Services, LLC provide information technology services to health care providers. We are writing to inform you of a data security incident involving some of your information in connection with the services provided to you by [redacted]. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

We recently determined that intermittent unauthorized access to our network occurred between January 19, 2022 and March 17, 2022.

What We Are Doing.

Upon learning of this issue, we immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to assess the extent of any compromise. After an extensive investigation, we concluded on May 18, 2022 that an unauthorized party potentially removed a limited number of files and folders from our system that may contain your personal information.

What Information Was Involved?

The acquired files potentially contained your [redacted].

What You Can Do.

We want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary [redacted]-year membership of identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: [redacted] months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on your complimentary [redacted]-year membership, please see the additional information provided in this letter.

This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 6 am to 6 pm Pacific Time.

Sincerely,

Avamere Health Services, LLC

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [redacted] Month Credit Monitoring.

Activate IDX Identity Protection Membership Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the IDX website to enroll: https://response.idx.us/avamere
3. PROVIDE the Enrollment Code: [redacted]

If you have questions about the product or if you would like to enroll over the phone, please contact IDX at [redacted].

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary [redacted]-month credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

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

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

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

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

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.