MOSES/WEITZMAN
Health System
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/MosesWeitzmanHealthSystem

January 30, 2025

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

You are receiving this letter because you are a current or former employee of Moses/Weitzman Health System, Inc. ("MWHS") or one of its affiliates: the Community eConsult Network, Inc., Community Health Center, Inc., National Institute for Medical Assistant Advancement, Inc. or National Nurse Practitioner Residency and Fellowship Training Consortium, Inc. (a/k/a Consortium for Advanced Practice Providers) (collectively, "Affiliates"). We are writing to inform you of a data security incident that may have exposed your personal information. Because the confidentiality of your data is one of our top priorities, we are providing you with information about the incident and steps you can take to protect your personal information.

What Happened

On January 2, 2025, MWHS staff became aware of unusual activity within our information systems. That same day, we retained a leading independent forensics firm to conduct a thorough investigation and reinforce the security of our systems. The investigation concluded that a sophisticated criminal actor had accessed the MWHS IT environment and successfully acquired some MWHS data, possibly including your personal information, and moved a copy of it out of the environment to a location controlled by the criminal actor. The criminal actor did not delete or encrypt any MWHS data and the incident did not have any significant impact on MWHS operations. We believe that we stopped the criminal actor's access within hours of discovering it and that there is no ongoing threat to MWHS.

Fortunately, MWHS's HR system for MWHS and Affiliate employee data was not compromised. As a result, there was no access to or acquisition of any data from that system such as Social Security Number, date of birth, address, compensation, direct deposit, offer letter, or performance information. Rather, some HR files regarding benefits information and very limited credentialing information may have been acquired. While those files do not include information on all (or even most) current or former employees, we are providing notice and identity theft prevention services to all such employees out of an abundance of caution and to expedite notification.

Finally, we have reason to believe that the criminal actor may have acquired information from the server containing employee network storage (known internally as your "F: Drive").

What Information Was Involved

If benefits information about you was involved, it may have included your name, date of birth, Social Security Number, health insurance information, and dependent information.

If you are a licensed or certified contractor who is receiving this letter, we have reason to believe that the personal information includes your name, address, month and day of birth (no year), license or certification information, the last four digits of your Social Security Number and a copy of the government-issued ID you provided (e.g., driver's license or passport).

To the extent that you have personal information in your F: Drive folder, such information also may have been involved.

What We Are Doing

In addition to the forensic investigation and the existing extensive security measures, we also deployed sophisticated software to each of our endpoints to monitor the environment for any suspicious activity. We are also taking additional steps to protect data from theft or similar criminal activity in the future.

We have no indication at this time that any of your personal information has been misused. Nevertheless, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 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.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by scanning the QR code above, calling 1-877-227-1846, or going to https://response.idx.us/MosesWeitzmanHealthSystem and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is April 30, 2025.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-877-227-1846 or go to https://response.idx.us/MosesWeitzmanHealthSystem for assistance or for any additional questions you may have.

We sincerely regret any inconvenience resulting from this criminal activity and thank you for your continued support of MWHS.

Peace and Health,

Mark Masselli
President and CEO
Moses/Weitzman Health System, Inc.

(Enclosure)

IDX
A ZEROFOX COMPANY

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://response.idx.us/MosesWeitzmanHealthSystem and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-877-227-1846 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receiveconfirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place

the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Connecticut Residents: The Attorney General may be contacted at: 165 Capitol Avenue, Hartford, CT 06106; 1-860-808-5318; https://portal.ct.gov/AG**.**

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov**.**

Iowa Residents: You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319**.**

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the 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 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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can 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.

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/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

Vermont Residents: 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 Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

MOSES/WEITZMAN
Health System
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/MosesWeitzmanHealthSystem

January 30, 2025

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

You are receiving this letter because you are or were a dependent or spouse of a current or former employee of Moses/Weitzman Health System, Inc. ("MWHS") or one of its affiliates: the Community eConsult Network, Inc., Community Health Center, Inc., National Institute for Medical Assistant Advancement, Inc. or National Nurse Practitioner Residency and Fellowship Training Consortium, Inc. (a/k/a Consortium for Advanced Practice Providers) (collectively, "Affiliates"). We are writing to inform you of a data security incident that may have exposed your personal information. Because the confidentiality of your data is one of our top priorities, we are providing you with information about the incident and steps you can take to protect your personal information.

What Happened

On January 2, 2025, MWHS staff became aware of unusual activity within our information systems. That same day, we retained a leading independent forensics firm to conduct a thorough investigation and reinforce the security of our systems. The investigation concluded that a sophisticated criminal actor had accessed the MWHS IT environment and successfully acquired some MWHS data, possibly including your personal information, and moved a copy of it out of the environment to a location controlled by the criminal actor. The criminal actor did not delete or encrypt any MWHS data and the incident did not have any significant impact on MWHS operations. We believe that we stopped the criminal actor's access within hours of discovering it and that there is no ongoing threat to MWHS.

What Information Was Involved

The personal information involved relates to your status as a dependent or spouse of a MWHS or Affiliate employee and includes your name, date of birth, Social Security Number, health insurance information, and relationship to the employee.

What We Are Doing

In addition to the forensic investigation and the existing extensive security measures, we also deployed sophisticated software to each of our endpoints to monitor the environment for any suspicious activity. We are also taking additional steps to protect data from theft or similar criminal activity in the future.

We have no indication at this time that any of your personal information has been misused. Nevertheless, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 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.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by scanning the QR code above, calling 1-877-227-1846, or going to https://response.idx.us/MosesWeitzmanHealthSystem and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is April 30, 2025.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-877-227-1846 or go to https://response.idx.us/MosesWeitzmanHealthSystem for assistance or for any additional questions you may have.

We sincerely regret any inconvenience resulting from this criminal activity and thank you for your continued support of MWHS.

Peace and Health,

Mark Masselli
President and CEO
Moses/Weitzman Health System, Inc.

(Enclosure)

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://response.idx.us/MosesWeitzmanHealthSystem and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-877-227-1846 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place

the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Connecticut Residents: The Attorney General may be contacted at: 165 Capitol Avenue, Hartford, CT 06106; 1-860-808-5318; https://portal.ct.gov/AG**.**

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov**.**

Iowa Residents: You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319**.**

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the 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 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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can 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.

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/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

Vermont Residents: 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 Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

MOSES/WEITZMAN
Health System
P.O. Box 989728
West Sacramento, CA 95798-9728

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/MosesWeitzmanHealthSystem

January 30, 2025

Notice of Data Breach

Dear Parent or Guardian of <<First Name>> <<Last Name>>,

You are receiving this letter because your child is a dependent of a current or former employee of Moses/Weitzman Health System, Inc. ("MWHS") or one of its affiliates: the Community eConsult Network, Inc., Community Health Center, Inc., National Institute for Medical Assistant Advancement, Inc. or National Nurse Practitioner Residency and Fellowship Training Consortium, Inc. (a/k/a Consortium for Advanced Practice Providers) (collectively, "Affiliates"). We are writing to inform you of a data security incident that may have exposed your child's personal information. Because the confidentiality of your child's data is one of our top priorities, we are providing you with information about the incident and steps you can take to protect your child's personal information.

What Happened

On January 2, 2025, MWHS staff became aware of unusual activity within our information systems. That same day, we retained a leading independent forensics firm to conduct a thorough investigation and reinforce the security of our systems. The investigation concluded that a sophisticated criminal actor had accessed the MWHS IT environment and successfully acquired some MWHS data, possibly including your personal information, and moved a copy of it out of the environment to a location controlled by the criminal actor. The criminal actor did not delete or encrypt any MWHS data and the incident did not have any significant impact on MWHS operations. We believe that we stopped the criminal actor's access within hours of discovering it and that there is no ongoing threat to MWHS.

What Information Was Involved

The personal information involved relates to your child's status as a dependent or spouse of a MWHS or Affiliate employee and includes your child's name, date of birth, Social Security Number, health insurance information, and relationship to the employee.

What We Are Doing

In addition to the forensic investigation and the existing extensive security measures, we also deployed sophisticated software to each of our endpoints to monitor the environment for any suspicious activity. We are also taking additional steps to protect data from theft or similar criminal activity in the future.

We have no indication at this time that any of your child's personal information has been misused. Nevertheless, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services

expert. IDX identity protection services include: 24 months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by scanning the QR code above, calling 1-877-227-1846, or going to https://response.idx.us/MosesWeitzmanHealthSystem and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is April 30, 2025.

Again, at this time, there is no evidence that your child's information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your child's personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-877-227-1846 or go to https://response.idx.us/MosesWeitzmanHealthSystem for assistance or for any additional questions you may have.

We sincerely regret any inconvenience resulting from this criminal activity and thank you for your continued support of MWHS.

Peace and Health,

Mark Masselli
President and CEO
Moses/Weitzman Health System, Inc.

(Enclosure)

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://response.idx.us/MosesWeitzmanHealthSystem and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at 1-877-227-1846 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

3. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Security Freeze. You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files.

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can 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.

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/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.