25854

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>>:

This letter serves as notification from **Medical Healthcare Solutions, Inc. (MHS)**, which provides surgical billing services to physician groups, that a recent cyber incident by an unauthorized individual on our network may have affected the privacy of some of your Protected Health Information (PHI). The privacy and security of the personal information we maintain is of the utmost importance to MHS. We are providing the following details of the incident and steps taken to provide you with increased protection and ongoing support.

What Happened? On November 19, 2021, MHS discovered that an unauthorized party removed certain files from our network between October 1 and 4, 2021. After an extensive forensic investigation, on January 8, 2022, MHS identified a final list of impacted PHI, which included your information.

What We Are Doing. MHS immediately locked down our network data system, launched a comprehensive investigation utilizing third-party computer specialists, and notified law enforcement. MHS has since stabilized and reopened the network, and implemented additional security measures to further protect our data system.

What Information Was Involved? The impacted PHI data may have included your name and the following information from medical care that you received from the physicians group <<Entity>>. The impacted PHI includes: <<Data Elements>>.

<<Entity>> provides physician services at the following hospitals where you may have received care, including but not limited to: Beth Israel Deaconess Medical Center, Beth Israel Deaconess Hospital – Plymouth, Beth Israel Deaconess Hospital – Needham, Beth Israel Deaconess Hospital – Milton, Anna Jaques Hospital, and Mount Auburn Hospital.

What You Can Do. MHS is providing potentially impacted individuals free access to 24 months of credit monitoring and identity protection services. Information about how to enroll in these services is included in the attached *Steps You Can Take To Protect Your Information*. This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert or Security Freeze on your credit files, and obtaining a free credit report. In addition, we are offering best practices to protect your medical information.

For More Information. Protecting the privacy of PHI is the top priority for MHS. We apologize for any concerns this situation may have caused you. We will continue to take every precaution to protect your personal information, and support your ability to monitor and protect your information moving forward.

MHS has also established a dedicated assistance line at **855-675-3125**, 9am – 9pm Eastern Time, Monday through Friday (excluding major U.S. holidays), or you may write to us at P.O. Box 3160, Andover, MA 01810-0803.

Sincerely,

Medical Healthcare Solutions, Inc.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

We encourage you to always remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms 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, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

1. Enroll in Credit Monitoring / Identity Protection

Enrollment Instructions

Go to ***www.equifax.com/activate*** and enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **Register:** Complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications when your personal information, such as Social Security number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft (conditions apply).

2. Place a Fraud Alert or Security Freeze on Your Credit File

You have the right to place an initial or extended **fraud alert** on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a **credit freeze** on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

3. Protect 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.

4. Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. MHS may be contacted at P.O. Box 3160, Andover, MA 01810-0803.

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection. MHS may be contacted at P.O. Box 3160, Andover, MA 01810-0803.

Medical Healthcare Solutions, Inc.

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

<<Mail ID>>
Parent/Guardian of
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear Parent/Guardian of <<Name 1>>:

This letter serves as notification from **Medical Healthcare Solutions, Inc. (MHS)**, which provides surgical billing services to physician groups, that a recent cyber incident by an unauthorized individual on our network may have affected the privacy of some of your minor's Protected Health Information (PHI). The privacy and security of the personal information we maintain is of the utmost importance to MHS. We are providing the following details of the incident and steps taken to provide you with increased protection and ongoing support.

What Happened? On November 19, 2021, MHS discovered that an unauthorized party removed certain files from our network between October 1 and 4, 2021. After an extensive forensic investigation, on January 8, 2022, MHS identified a final list of impacted PHI, which included your minor's information.

What We Are Doing. MHS immediately locked down our network data system, launched a comprehensive investigation utilizing third-party computer specialists, and notified law enforcement. MHS has since stabilized and reopened the network, and implemented additional security measures to further protect our data system.

What Information Was Involved? The impacted PHI data may have included your minor's name and the following information from medical care that your minor received from the physicians group <<Entity>>. The impacted PHI includes: <<Data Elements>>.

<<Entity>> provides physician services at the following hospitals where your minor may have received care, including but not limited to: Beth Israel Deaconess Medical Center, Beth Israel Deaconess Hospital – Plymouth, Beth Israel Deaconess Hospital – Needham, Beth Israel Deaconess Hospital – Milton, Anna Jaques Hospital, and Mount Auburn Hospital.

What You Can Do. MHS is providing potentially impacted individuals access to 24 months of identity protection services. Information about how to enroll in these services is included in the attached *Steps You Can Take To Protect Your Minor's Information*. This letter also provides other precautionary measures you can take to protect your minor's personal information.

For More Information. Protecting the privacy of PHI is the first priority of MHS. We apologize for any concerns this situation may have caused you. We will continue to take every precaution to protect personal information, and support your ability to monitor and protect your minor's information moving forward.

MHS has also established a dedicated assistance line at **855-675-3125**, 9am – 9pm Eastern Time, Monday through Friday (excluding major U.S. holidays), or you may write to us at P.O. Box 3160, Andover, MA 01810-0803.

Sincerely,

Medical Healthcare Solutions, Inc.

STEPS YOU CAN TAKE TO PROTECT YOUR MINOR'S INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor's account statements and your explanation of benefits forms for suspicious activity and to detect errors. Although minors typically do not have a credit report, under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

1. Enroll in Identity Protection

Enrollment Instructions

Parent/guardian go to ***www.equifax.com/activate.*** Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **Register:** Complete the form with parent/guardian contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:** Enter parent/guardian email address, create a password, and to accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of parent/guardian identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling.
   The confirmation page shows parent/guardian completed enrollment.
   Click "View My Product" to access the product features and enroll minor children.

Key Features

- Child Monitoring for up to four children under the age of 18
- Emailed notifications to the primary adult member of activity on the child's Equifax credit report

2. Place a Credit Freeze on Your Minor's Credit File

You have the right to place a **credit freeze** on your minor's file, which will prohibit a credit bureau from releasing information in the credit file without your express authorization. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on a credit file. To request a credit freeze for your minor, you will need to provide the following information for both you and your minor:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth; and
4. Address for the prior two to five years.

Include for your identification:

5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. Proof that you are the parent or legal guardian of the minor.

Include for your minor's identification:

8. A copy of your minor's Social Security card; and
9. A copy of your minor's birth certificate.

Should you wish to contact the credit reporting bureaus or place a credit freeze, please contact the bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Security Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Security Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Security Freeze** P.O. Box 105788 Atlanta, GA 30348

3. Protect Your Medical Information.

We have no evidence that your minor's 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 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.

4. Additional Information

You can further educate yourself regarding identity theft, credit freezes, and the steps you can take to protect your minor's personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if your minor experiences 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 your minor has been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. MHS may be contacted at P.O. Box 3160, Andover, MA 01810-0803.

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection. MHS may be contacted at P.O. Box 3160, Andover, MA 01810-0803.

Medical Healthcare Solutions Notice of Cyber Incident
January 21, 2022

Andover, MA – Medical Healthcare Solutions, Inc. (MHS), recently experienced a cyber-incident that impacted some protected health information (PHI) within its data network. MHS immediately shut down its data system, conducted an extensive investigation, notified law enforcement, and implemented additional security measures. On November 19, 2021, MHS discovered the unauthorized party may have removed files from its network. On January 8, 2022, MHS identified a final list of impacted PHI, and on January 21, 2022, sent notifications by mail to impacted individuals.

Some of the impacted information may have included: name, address, date of birth, sex, phone number, email address, Social Security number, driver's license/state ID number, financial account number, routing number, payment card number, card CVV/expiration, diagnosis/treatment information, procedure type, provider name, prescription information, date of service, medical record number, patient account number, insurance ID number, insurance group number, claim number, insurance plan name, provider ID number, procedure code, treatment cost, and diagnosis code. MHS is issuing this notice on behalf of its clients, Harvard Medical Faculty Physicians at Beth Israel Deaconess Medical Center and Associated Physicians of Harvard Medical Faculty Physicians at Beth Israel Deaconess Medical Center.

The privacy and security of the personal information MHS maintains on behalf of its clients is of the utmost importance. MHS has established a dedicated assistance line for impacted individuals with questions or concerns at **855-675-3125**, Monday through Friday, (except U.S. holidays), from 9 a.m. – 9 p.m., EST, or by mail at P.O. Box 3160, Andover, MA 01810-0803. In addition, MHS is offering impacted individuals up to 24 months of credit monitoring and identity protection services.

Notified individuals should take actions to help protect their information by remaining vigilant in reviewing their account and explanation of benefits statements and consider placing a fraud alert and/or security freeze on their accounts.

Notice of Cyber Incident

January 21, 2022

Medical Healthcare Solutions, Inc. (MHS), recently experienced a cyber-incident that impacted some protected health information (PHI) within its data network. MHS immediately shut down its data system, conducted an extensive investigation, notified law enforcement, and implemented additional security measures. On November 19, 2021, MHS discovered the unauthorized party may have removed files from its network. On January 8, 2022, MHS identified a final list of impacted PHI, and on January 21, 2022, sent notifications by mail to impacted individuals.

Some of the impacted information may have included: name, address, date of birth, sex, phone number, email address, Social Security number, driver's license/state ID number, financial account number, routing number, payment card number, card CVV/expiration, diagnosis/treatment information, procedure type, provider name, prescription information, date of service, medical record number, patient account number, insurance ID number, insurance group number, claim number, insurance plan name, provider ID number, procedure code, treatment cost, and diagnosis code. MHS is issuing this notice on behalf of its clients, Harvard Medical Faculty Physicians at Beth Israel Deaconess Medical Center and Associated Physicians of Harvard Medical Faculty Physicians at Beth Israel Deaconess Medical Center.

The privacy and security of the personal information MHS maintains on behalf of its clients is of the utmost importance. MHS has established a dedicated assistance line for impacted individuals with questions or concerns at **855-675-3125**, Monday through Friday, (except U.S. holidays), from 9 a.m. – 9 p.m., EST, or by mail at P.O. Box 3160, Andover, MA 01810-0803. In addition, MHS is offering impacted individuals up to 24 months of credit monitoring and identity protection services.

Notified individuals should take actions to help protect their information by remaining vigilant in reviewing their account and explanation of benefits statements and consider placing a fraud alert and/or security freeze on their accounts.