uchealth

November 13th, 2026

RE: NOTICE OF DATA BREACH

[redacted]

SIMID 210

[redacted]

Dear [redacted]:

UCHealth, including its affiliated healthcare facilities (collectively, "UCHealth"), values and respects the privacy of your information, which is why we are writing to inform you of a data security incident that may have involved some of your personal information. We have no evidence that your personal information has been misused. Nonetheless, we want you to be aware of the incident and to have guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On July 27, 2026, we discovered that an unauthorized third party gained access to two employee accounts in UCHealth's Microsoft cloud system. As soon as this was discovered, UCHealth launched an internal investigation, secured the affected accounts and system from further unauthorized access, and notified law enforcement of the incident. Our investigation determined that the unauthorized activity was limited to certain services within the cloud system and that the unauthorized third party may have acquired certain files stored there. Importantly, UCHealth's electronic health record was not accessed.

What Information Was Involved? We reviewed the files involved to determine if they contained any personal information and recently determined that the files may have included your name, Social Security number, health information, and/or billing information. Your personal banking and credit card information was not involved.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. Although we have no evidence that your information has been used for identity theft or fraud, we have arranged for you to enroll in a two-year membership in Medical Shield Total, if you would like to do so. This product helps enrollees detect possible misuse of their personal information and provides identity protection services focused on prompt identification and resolution of identity theft. Medical Shield Total is completely free to you. **For more information, including instructions on how to activate your complimentary membership, please refer to the additional information enclosed.**

What You Can Do. We encourage you to take advantage of the complimentary credit monitoring. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience this incident might cause. If you need assistance or additional information, please call [redacted] from Monday – Friday 8 a.m. to 11 p.m. and Saturday 9 a.m. to 6 p.m. ET, except holidays, to speak with a representative specially trained to answer questions about the incident and this notice.

Sincerely,

UCHealth

MEDICAL SHIELD

Service Term: **24 Months***

Medical Shield Total

Key Features

- 3-Bureau Credit Monitoring
- Health Insurance Plan Number Monitoring
- Medical Record Number Monitoring
- Medical Beneficiary Identifier Monitoring
- National Provider Number Monitoring
- International Classification of Diseases Monitoring
- Health Savings Account Monitoring
- Dark Web Monitoring
- Victim Assistance
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Medical Shield, visit [redacted]

1. **Enter your unique Activation Code** [redacted]
   Enter your Activation Code and click “Redeem Code”.
2. **Create Your Account**
   Enter your email address, create your password, and click “Create Account”.
3. **Register**
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click “Complete Account”.
4. **Complete Activation**
   Click “Continue to Dashboard” to finish enrolling.

The deadline to enroll is [redacted]. After [redacted], the enrollment process will close, and your Medical Shield code will no longer be active. If you do not enroll by [redacted], you will not be able to take advantage of Medical Shield, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Medical Shield, please call Medical Shield directly at [redacted].

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Under Massachusetts law, you have the right to obtain any police report filed 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.

The District of Columbia and Massachusetts law also allow consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/ P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze 1-888-397-3742 https://www.experian.com/freeze/center.html P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze 1-888-909-8872 https://www.transunion.com/credit-freeze P.O. Box 160 Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:
1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you
to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action. Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Washington, DC Residents: Washington, DC residents can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.