MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

3001 N. Rocky Point Drive East, Suite 200
Tampa, FL 33607

March 26, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We represent INTEGRIS Health, Inc. ("INTEGRIS Health") located at 3001 Quail Springs Parkway, Oklahoma City, Oklahoma 73134. We are writing to supplement our notice to your office on February 6, 2024, and provide notice on behalf of INTEGRIS Health Community Hospitals ("IH Community Hospitals"). By providing this supplemental notice, INTEGRIS Health does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

At the time the initial round of notification letters were mailed to potentially affected individuals, INTEGRIS Health was still completing its data mining and identifying any remaining notice population, and contact information for those individuals. This additional review was completed on February 21, 2024, and INTEGRIS Health provided notice to the impacted individuals on March 1, 2024.

INTEGRIS Health has now completed its review of the potentially impacted data and determined that the potentially impacted population includes patients of IH Community Hospitals. As a result, the following are the IH Community Hospitals on behalf of whom INTEGRIS Health has provided notice:

As we previously reported, on or about February 6, 2024, INTEGRIS Health began providing written notice of this incident to affected individuals. On March 26, 2024, INTEGRIS Health provided notice to one (1) additional New Hampshire resident related to IH Community Hospitals. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

INTEGRIS Health is providing access to credit monitoring services for twenty-four (24) months through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, INTEGRIS Health is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. INTEGRIS Health is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

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

Very truly yours,

Kevin M. Mekler of
MULLEN COUGHLIN LLC

KMK/kgl
Enclosure

EXHIBIT A

INTEGRIS HEALTH

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

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

March 26, 2024

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

INTEGRIS Health is writing on behalf of INTEGRIS Health Community Hospitals ("IH Community Hospitals") to notify you of an incident that may have impacted the security of your personal information from care you received at one of the IH Community Hospitals. We want to provide you with information about the incident, our response, and steps you may take to further safeguard your personal information should you feel it necessary to do so.

Why Are You Receiving this Notice from INTEGRIS Health? Besides operating healthcare facilities across Oklahoma, INTEGRIS Health provides electronic health record support to IH Community Hospitals. If you are receiving this notice, it means that you received care at one of the IH Community Hospitals. If you already received notice from INTEGRIS Health, this is **not a new or additional incident**; it just means that you received care from both IH Community Hospitals and another INTEGRIS Health location where your personal information was involved.

What Happened? INTEGRIS Health detected suspicious activity within its environment. Upon becoming aware of the suspicious activity, INTEGRIS Health promptly took steps to secure the environment and commence an investigation into the nature and scope of the unauthorized activity. The investigation determined that a file was accessed by an unauthorized party on or about November 28, 2023. INTEGRIS Health then initiated a thorough forensic review to determine the type of information, to whom it related and which healthcare entities were involved. As that review was ongoing, on December 24, 2023, INTEGRIS Health learned that some INTEGRIS Health patients received communications from a group claiming responsibility for the unauthorized access.

Why Are You Getting Notified Now? As a result of its thorough forensic review, INTEGRIS Health determined on or about January 29, 2024 that patient information from IH Community Hospital locations were also included in the accessed files and notified the IH Community Hospitals. INTEGRIS Health is now notifying you on behalf of the following IH Community Hospitals that patient information from these hospitals was also involved:

What Information Was Involved? The investigation determined that your name and the following types of personal information were present in the files accessed or acquired by the unauthorized actor at the time of the incident:

This incident does NOT involve credit card or other financial/payment information, employment information, driver's license, or access or the password to your electronic health record.

What We are Doing. Upon learning of this incident, INTEGRIS Health promptly assessed the security of its systems, engaged third-party cybersecurity specialists, and implemented security enhancements, including reviewing existing policies and procedures to reduce the likelihood of a similar future incident. INTEGRIS Health continues to monitor its systems and has not observed any further unauthorized activity within its systems and believes that the incident has been contained. As a precautionary measure, we are notifying potentially affected individuals, including you, and to provide peace of mind, offering complementary identity theft and credit monitoring so you may take further steps to better protect your personal information should you feel it is appropriate to do so. These services help detect suspicious activity related to your personal information and provide support in case of identity theft.

What You Can Do. INTEGRIS Health and IH Community Hospitals encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the attached *"Steps You Can Take to Protect Your Personal Information."*

While we believe the threat is now contained, if you receive any communication from a group claiming responsibility for the unauthorized access, **we urge you to NOT respond to any communication from the sender or follow any instructions, including accessing any links.** Instead, please see the steps in the *"Steps You Can Take to Protect Your Personal Information."* below.

For More Information. As a result of this incident, INTEGRIS Health partnered with IDX to provide you with notification and complementary access to credit monitoring and identity restoration services for as an added precaution. To enroll in these free services, you may call or go to https://app.idx.us/account-creation/protect or scan the QR image, and use the Enrollment Code provided above. Representatives are available Monday through Friday from 8:00 am – 8:00 pm Central Time. Please note the deadline to enroll is .

Again, we regret any inconvenience or concern this incident may cause.

Sincerely,

INTEGRIS Health on behalf of the Integris Health Community Hospitals

Steps You Can Take To Protect Your Personal Information

Enroll in Monitoring Services

1. **Website and Enrollment.** Scan the QR image or go to https://app.idx.us/account-creation/protect 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 (888) 447-8141 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. 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; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.

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 reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There is approximately 1 Rhode Island resident that may be impacted by this event.