

# **EXHIBIT 1**

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, INTEGRIS Health does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

### **Nature of the Data Event**

INTEGRIS Health discovered potential unauthorized activity on certain systems. Upon becoming aware of the suspicious activity, INTEGRIS Health promptly took steps to secure the environment and commenced an investigation into the nature and scope of the activity. The investigation determined that certain files were accessed or acquired by an unauthorized party on November 28, 2023. INTEGRIS Health initiated a thorough review of the data to determine the type of information and to whom it related, and just recently completed that effort.

The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, and medical information.

### **Notice to Washington Residents**

On or about February 6, 2024, INTEGRIS Health began providing written notice of this incident to two thousand twenty-five (2,025) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, INTEGRIS Health moved quickly to investigate and respond to the incident, assess the security of INTEGRIS Health systems, and identify potentially affected individuals. Further, INTEGRIS Health notified federal law enforcement regarding the event and is cooperating with their investigation. INTEGRIS Health is also working to implement additional safeguards and training to its employees. 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. INTEGRIS Health is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

INTEGRIS Health is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. INTEGRIS Health is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

# **EXHIBIT A**



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:



Or Visit:

<https://app.idx.us/account-creation/protect>

February 6, 2024

## NOTICE OF DATA BREACH

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

INTEGRIS Health is writing to notify you of an incident that may have impacted the security of your personal information. We want to provide you with information about the incident, our response, and steps you may take to better protect yourself against possible misuse of your personal information, should you feel it is necessary to do so. As a result of this incident, we have partnered with IDX to provide you with this notification.

**What Happened?** INTEGRIS Health discovered potential unauthorized activity on certain systems. Upon becoming aware of the suspicious activity, INTEGRIS Health promptly took steps to secure the environment and commenced an investigation into the nature and scope of the activity. The investigation determined that certain files may have been accessed by an unauthorized party on November 28, 2023. INTEGRIS Health initiated a thorough review of the potentially accessed data to determine the type of information and to whom it related, and just recently completed that effort.

As that review was ongoing, on December 24, 2023, INTEGRIS Health learned that some patients began receiving communications from a group claiming responsibility for the unauthorized access. We encourage anyone receiving such communications to NOT respond or contact the sender or follow any of the instructions. Instead, please see the steps in the What You Can Do section below.

**What Information Was Involved?** The investigation determined that your name and the following types of personal information were present in the files accessed and/or acquired by the unauthorized actor at the time of the incident: name, <<data elements>>. This does NOT involve Employment information, Driver's License, Financial/Payment Information, or username/password.

**What We Are Doing.** We take this incident and the security of personal information in our care very seriously. Upon learning of this incident, we initiated an investigation with the assistance of third-party cybersecurity specialists, assessed the security of our systems and notified potentially affected individuals. As part of our ongoing commitment to the security of information, we are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future incident. As a precautionary measure, we are notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so.

**What You Can Do.** We 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.”*

**For More Information.** We regret any inconvenience or concern this incident may cause. As an added precaution, we are offering access to 24 months of credit monitoring and identity theft protection services through IDX, at no cost to you. To enroll in free identity protection services you may call (888) 447-8141 or go to <https://app.idx.us/account-creation/protect> or scan the QR image, and use the Enrollment Code provided below. Representatives are available Monday through Friday from 8:00 am – 8:00 pm Central Time. Please note the deadline to enroll is May 9, 2024.

Sincerely,

INTEGRIS Health

## 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](http://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.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. 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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
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](http://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 District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and [oag.dc.gov](http://oag.dc.gov).

*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](http://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](http://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](http://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 are approximately 95 Rhode Island residents that may be impacted by this event.