MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

July 16, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Intermountain Healthcare ("Client") located at 36 S State St, Salt Lake City, Utah 84111, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. 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, Client 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.

Nature of the Data Event

On or about May 17, 2021, Intermountain Healthcare received notice from Elekta, its business associate, that a server with some data relating to Intermountain Healthcare's patients was affected in a data security incident that impacted certain Elekta systems. Elekta reported on or around April 6, 2021, that it had been the victim of a data security incident. On May 17, 2021, Elekta confirmed that this incident resulted in certain PHI stored on the impacted systems becoming accessible to unauthorized person(s) between April 6, 2021 and April 20, 2021. Upon receiving this notification, Intermountain Healthcare immediately worked with Elekta and others to confirm the nature and scope of the data at issue, including whether and how it related to patients of Intermountain Healthcare.

Unfortunately, the Client cannot confirm if any specific information related to the impacted individuals was actually accessed or viewed by an unauthorized person as a result of the Elekta incident. However, Elekta's investigation determined that the data present on their impacted

systems at the time of the incident included patient's name and scanned image files. The scanned image files could have included medical images, and information on medical intake forms. The patients may have provided their Social Security number, date of birth, demographic information, insurance card, and other identification cards.

Notice to New Hampshire Resident

On or about July 16, 2021, Client provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. 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, Client moved quickly to investigate and respond to the incident, assess the security of Client systems, and notify potentially affected individuals. Client is working with Elekta to implement additional safeguards. Elekta also migrated Client's data to a new-generation cloud system as part of Elekta's commitment to safeguarding customer data. Client is providing access to credit monitoring services for 1 or 2 year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Client 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. Client 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/crm

EXHIBIT A

Intermountain Healthcare

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>> <<Name 2>>:

We are writing to inform you of a data security incident experienced by Elekta, a vendor that provides cloud-based storage for Intermountain Healthcare[1] and houses certain patient's data. This incident may have involved your protected health information and, as a precaution, we are providing details about the incident and steps you can take to help protect your information. We take the privacy and security of your protected health information very seriously and we sincerely regret any concern this incident may cause you.

What Happened? On April 6, 2021, we received notice from Elekta that it experienced a data security incident that impacted certain Elekta systems. Upon receiving this notification, we immediately worked with Elekta and others to confirm the nature and scope of the data at issue, including whether and how it related to patients of Intermountain Healthcare. Elekta further reported that this incident resulted in certain PHI stored on the impacted systems becoming accessible to unauthorized person(s) between April 6, 2021 and April 20, 2021. On May 17, 2021, Elekta reported that a server with some data relating to Intermountain Healthcare patients was affected. This data indicated that information related to you was present on the impacted Elekta systems at the time of the incident. We promptly evaluated the data received and took additional steps to identify affected individuals such as yourself.

What Information Was Involved? We cannot confirm if any specific information relating to you was actually accessed or viewed by an unauthorized person as a result of the Elekta incident. However, Elekta's investigation determined that the data present on their impacted systems at the time of the incident included your name and scanned image files. The scanned image files could have included medical images, and information on medical intake forms. If you filled out an intake form, you may have provided your Social Security number, date of birth, demographic information, insurance card, and other identification cards. After a thorough investigation, we are unfortunately unable to determine the specificity of information contained on the scanned image files corresponding with the patient's name. Please note, there is currently have no evidence of misuse related to your information and we are informing you as a precautionary measure.

What We Are Doing. The privacy of those we serve is very important to us. Upon learning of this incident, we worked closely with Elekta to respond and determine the impact to Intermountain Healthcare's data and you. We understand that Elekta partnered with cybersecurity specialists to launch an investigation into this incident and mitigate any potential harm. We further understand from Elekta that Intermountain Healthcare users were migrated to a new-generation cloud system as part of Elekta's commitment to safeguarding Intermountain Healthcare's data. As part of our ongoing commitment to protect the information in our care, we are working to review our existing policies and procedures as they pertain to third-party vendors and working with Elekta to evaluate additional measures and safeguards to better protect against this type of incident in the future.

---

[1] Healthcare Partners Nevada, an Intermountain Healthcare company, is also the custodian of medical records transferred in the June 1, 2013 purchase of Nevada Cancer Center, Nagy, PLLC ("Nagy, PLLC"). The Asset Purchase Agreement was with Nagy, PLLC and M. Nafees Nagy, M.D.

As an added precaution, we are also offering you access to 12 months of complimentary credit monitoring and identity restoration services through Experian. Although these services are being offered to you free of cost, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions below.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and credit reports for suspicious activity and to detect errors. You can learn more about how to protect yourself generally against the possibility of theft or misuse of personal information in the enclosed document, "Steps You Can Take to Protect Information." There, you will find more information about the credit monitoring services we are offering and how to enroll.

For More Information. We understand that you may have questions about the Elekta incident that are not addressed in this letter. To ensure your questions are answered in a timely and sufficient manner, please call 866-281-0520, Monday through Friday from 9:00 a.m. to 11:00 p.m., and Saturday and Sunday from 11:00 a.m. to 8:00 p.m., excluding national holidays.

We apologize for any inconvenience or concern this incident may cause you.

Sincerely,

Suzanne Draper
VP, Compliance and Business Ethics
Intermountain Healthcare

STEPS YOU CAN TAKE TO PROTECT INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering a complimentary [redacted] membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: [redacted] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [redacted]
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] by [redacted] Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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
888-298-0045	1-888-397-3742	833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your 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: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Intermountain Healthcare is located at 36 S State St, Salt Lake City, Utah 84111.

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, the consumer reporting bureaus 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 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. We encourage you to 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.

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, you have the right to obtain any police report filed in regard to this incident. There are [redacted] Rhode Island residents impacted by this incident.