MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

April 25, 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: Notice of Data Event**

Dear Sir or Madam:

We represent Falcon Healthcare, Inc. d/b/a Interim Healthcare of Lubbock Texas ("Falcon") located at 101 W. Renner Rd., Ste. 420, Richardson, Texas 75082, and write to notify your office of an event that may affect the security of certain information relating to New Hampshire residents. By providing this notice, Falcon 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

In June of 2022, Falcon identified suspicious activity on a limited portion of its network. Falcon undertook an extensive investigation, with the assistance of third-party cybersecurity and digital forensic specialists, to determine the nature and scope of the activity. Falcon also reported the event to federal law enforcement. Initial forensic analysis suggested the unauthorized activity was limited to a server maintaining internal company information. On or around August 10, 2022, the investigation determined that a limited number of systems containing information related to certain patients were accessed and downloaded by an unknown actor between April 29, 2022 and July 3, 2022.

Following completion of the forensic investigation, Falcon undertook a comprehensive data mining exercise with the assistance of third-party data review specialists to determine specifically what information was maintained on the impacted systems and to whom the information related. To ensure compliance with applicable regulations while the data review was ongoing, Falcon

notified its primary federal regulator, the U.S. Department of Health and Human Services and issued legal notice in prominent print media in Texas beginning on October 9, 2022. Following the third-party data mining exercise, Falcon engaged in a lengthy manual process that was later supplemented by external specialists, to locate address information to provide notice to all potentially affected individuals. This process was recently completed.

The personal information that could have been subject to unauthorized access for New Hampshire residents includes: .

**Notice to New Hampshire Residents**

As noted above, Falcon began providing initial notice of the event to potentially affected individuals on October 9, 2022, while the investigation was ongoing. On April 25, 2024, Falcon continued providing notice to potentially affected individuals, including approximately four (4) New Hampshire residents via written letter. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***. On April 25, 2024, Falcon also began providing updated substitute notice in prominent print media in Texas and New Mexico in substantially the same form as the notice attached hereto as ***Exhibit B.***

**Other Steps Taken and To Be Taken**

Upon becoming aware of the event, Falcon moved quickly to investigate and respond, assess the security of its systems, notify its primary federal regulator, and identify potentially affected individuals. Further, Falcon reported the event to federal law enforcement and cooperated with their investigation. Falcon is also working to implement additional administrative and technical safeguards, as well as further training to its employees. Falcon is providing access to credit monitoring and identity restoration services for , through Equifax, to individuals whose personal information was potentially affected by this event, at no cost to these individuals. Falcon also established a dedicated assistance telephone line to assist notified individual with questions regarding the event and complimentary services.

Additionally, Falcon is providing potentially affected 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. Falcon 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.

Falcon is providing written notice of this event to appropriate state privacy regulators, and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion. As noted, Falcon

also notified the U.S. Department of Health and Human Services and fully cooperated with its investigation.

**Contact Information**

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

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/crm
Enclosure

# EXHIBIT A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

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

<<Date>>

**<<Notice of Data Breach>>**

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

Falcon Healthcare, Inc. d/b/a Interim Healthcare of Lubbock Texas ("Falcon") writes to inform you of an event that may affect the confidentiality of certain information related to you. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so

**What Happened?** In June of 2022, we identified suspicious activity on a limited portion of its computer network. Falcon promptly undertook an extensive investigation, with the assistance of cybersecurity specialists, to determine the nature and scope of the activity. The investigation subsequently determined that information related to certain patients was accessed and downloaded by an unknown actor between April 29, 2022 and July 3, 2022. We reported this activity to federal law enforcement and government regulators.

We then conducted a comprehensive review of the affected systems, with the assistance of third-party data review specialists, to determine what information was contained within the systems and to whom the information related. Following the third-party review, we undertook a time-intensive manual review of the records to validate the information and identify address information to provide notifications. This review was recently completed.

**What Information Was Involved?** The information present within the impacted systems could have included your

.

**What We Are Doing**. We take this event and the security of information in our care seriously. Upon learning of the event, we moved quickly to investigate and respond, assess the security of our environment, and determine what information was potentially impacted. As part of our ongoing commitment to information security, we reviewed our existing policies and procedures, enhanced certain administrative and technical controls, and provided additional security training to reduce the likelihood of a similar future event. As an added precaution, we are offering complimentary credit monitoring and identity restoration services for <<12/24>> months through Equifax.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft by reviewing account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. Any suspicious activity should be promptly reported to your insurance company, health care provider, or financial institution. We also encourage you to review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*. In addition, you may enroll in the complimentary credit monitoring services available to you. Enrollment instructions are enclosed with this letter.

**For More Information.** If you have additional questions, you may call our designated assistance line at 888-841-3406 (toll-free) Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time (excluding U.S. holidays). You may also write to Falcon at 3305 101st St., Suite 200, Lubbock, TX 79423.

Sincerely,

Shelly Marker
Chief Executive Officer
Falcon Healthcare, Inc.

**STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION**

**Enroll in Credit Monitoring**

EQUIFAX®

<<FIRST NAME>> <<LAST NAME>>
**Enter your Activation Code:** *<<ACTIVATION CODE>>*
**Enrollment Deadline:** *<<ENROLLMENT DEADLINE>>*

## Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

## Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] 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[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- 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[4]

## Enrollment Instructions

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 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.

   **You're done!**
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

**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 one-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. You should be aware, however, 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 |
| 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 consumers can take to protect 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, 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. 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. 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 consumer's 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.

*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. Fees may be required to be paid to the consumer reporting agencies. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.

# EXHIBIT B

**Falcon Healthcare, Inc. d/b/a Interim Healthcare of Lubbock Texas Provides Updated Notice of Data Security Event**

Falcon Healthcare, Inc. d/b/a Interim Healthcare of Lubbock Texas ("Falcon") is providing updated notice of a data security event that potentially affected the confidentiality of information related to certain individuals.

In June of 2022, Falcon identified suspicious activity on a limited portion of its computer network. Falcon promptly undertook an extensive investigation, with the assistance of cybersecurity specialists, to determine the nature and scope of the activity. The investigation subsequently determined that information related to certain patients was accessed and downloaded by an unknown actor between April 29, 2022 and July 3, 2022. We reported this activity to federal law enforcement and government regulators.

Falcon then conducted a comprehensive review of the affected systems, with the assistance of third-party data review specialists, to determine what information was contained within the systems and to whom the information related. Following the third-party review, Falcon undertook a time-intensive manual review of the records to validate the information and identify address information to provide notifications. This review was recently completed.

The types of information that may have been present in the impacted systems during the event varies by individual and could have included:

.

Falcon is providing updated notifications via this media release and by mailing letters to potentially affected individuals. Falcon is also notifying appropriate government regulators. For individuals seeking additional information regarding this event, a toll-free assistance line has been established. Individuals may call the assistance line at Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 8:00 p.m., Central time.

As a precautionary measure, Falcon encourages potentially affected individuals to remain vigilant against incidents of identity theft by reviewing account statements, credit reports, and explanations of benefits for unusual activity and to detect errors. Any suspicious activity should be promptly reported to their insurance company, health care provider, or financial institution.

Falcon takes this event and the security of the information in its care very seriously. As part of Falcon's ongoing commitment to information security, Falcon worked to update a range of privacy and security safeguards designed to enhance its existing protections.

###