

Melissa K. Ventrone  
T (312) 360-2506  
F (312) 517-7572  
Email: mventrone@ClarkHill.com

Clark Hill  
130 E. Randolph Street, Suite 3900  
Chicago, Illinois 60601  
T (312) 985-5900  
F (312) 985-5999

March 4, 2022

Sent Via Online Submission

Office of the Attorney General  
6 State House Station  
Augusta, ME 04333

To Whom It May Concern:

We represent Duncan Regional Hospital, Inc. (“DRH”) with respect to a data security incident involving potential exposure of certain personal information for hospital patients and employees described in more detail below. DRH is a not-for-profit community hospital located in Duncan, Oklahoma that provides health care services to the community. DRH is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

**1. Nature of security incident.**

On January 20, 2022, DRH detected a data security incident that impacted access to some of its systems. DRH immediately disconnected all systems from external access, implemented its incident response protocols, and notified law enforcement. Under the direction of Outside Counsel, an independent computer forensics firm was hired to conduct a forensic investigation to determine how the incident occurred and whether any information may have been impacted.

The investigation determined that patient information and employee information may have been impacted as part of this incident. For patients, this may include name, date of birth, Social Security number, limited treatment information and medical appointment information such as date of service and name of providers. For employees, this includes personal information associated with W-2s, such as name, date of birth, address, and Social Security number.

**2. Number of residents affected.**

Four (4) Maine residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on March 4, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

**3. Steps taken in response to the incident.**

DRH took steps to address this incident and to prevent similar incidents in the future, including but not limited to changing all passwords, tightening firewall restrictions, and implementing endpoint threat detection and response monitoring software on workstations and servers. DRH secured the services of

March 4, 2022

Page 2

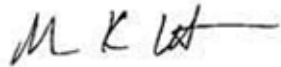
Experian to provide credit monitoring and identity protection services to impacted individuals. Notice will also be provided to the Department of Health and Human Services Office of Civil Rights.

**4. Contact information.**

DRH takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at [mventrone@clarkhill.com](mailto:mventrone@clarkhill.com) or (312) 360-2506.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read "M K Ventrone" with a horizontal line extending to the right.

Melissa K. Ventrone  
Member

cc: Daisy Dai [ddai@clarkhill.com](mailto:ddai@clarkhill.com)



Return Mail Processing  
 PO Box 589  
 Claysburg, PA 16625-0589

March 4, 2022

H6251-L02-0000002 T00001 P001 \*\*\*\*\*SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L02 PATIENT WITH SSN  
 APT ABC  
 123 ANY STREET  
 ANYTOWN, ST 12345-6789



### NOTICE OF DATA SECURITY INCIDENT

Dear Sample A. Sample,

DRH Health, also known as Duncan Regional Hospital, Inc. (“DRH”) is writing to let you know about a data security incident that may have impacted your protected health information (“PHI”). We take the privacy and security of your information seriously and sincerely apologize for any concerns or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

#### What happened:

On January 20, 2022, DRH detected a data security incident that impacted access to some of our systems. As soon as we learned about the incident, we immediately implemented our incident response protocols, disconnected all systems, and external cybersecurity experts were hired to conduct a forensic investigation. The investigation found that a limited amount of information stored outside our primary electronic medical records system may have been impacted. The privacy and security of your information is important to us, and we wanted to let you know about the incident out of an abundance of caution.

#### What information was involved:

Impacted information may include your name, [Extra1] [Extra2].

#### What we are doing:

We are taking steps in response to this incident to enhance the security of our systems, including changing all passwords, tightening firewall restrictions, and implementing endpoint threat detection and response monitoring software on workstations and servers.

In addition, to help protect your identity, we are offering a complimentary ##-month membership of Experian’s® IdentityWorks<sup>SM</sup>. 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: May 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

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 (888) 401-0543 by **May 31, 2022**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

0000002



H6251-L02

## ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 401-0543. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

### What you can do:

It is always a good idea to remain vigilant for incidents of identity theft or fraud, and review your estimate of benefits and contact your provider if you identify any errors. We also encourage you to contact Experian with any questions and to take full advantage of their service offering. Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

### For more information:

If you have any questions or concerns, please call (888) 401-0543 Monday through Friday from 8 a.m. to 10 p.m. Central, and Saturday and Sunday from 10 a.m. to 7 p.m. Central. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,



Jay R. Johnson  
President and Chief Executive Officer  
DRH Health

## RECOMMENDED STEPS TO PROTECT YOUR INFORMATION

**1. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**2. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
P.O. Box 105069  
Atlanta, GA 30348-5069

Equifax Credit Freeze  
P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-836-6351

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian Fraud Reporting and  
Credit Freeze  
P.O. Box 9554  
Allen, TX 75013

1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
P.O. Box 2000  
Chester, PA 19022-2000

TransUnion Credit Freeze  
P.O. Box 160  
Woodlyn, PA 19094  
1-800-680-7289

[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**3. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**4. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.



**District of Columbia:** Office of the Attorney General, 400 6<sup>th</sup> Street, NW, Washington, DC 20001; 202-727-3400; [oag@dc.gov](mailto:oag@dc.gov).

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**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 agencies 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 a 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201904\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201904_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.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392.

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)