SpencerFane

Shawn E. Tuma
Direct Dial: 972.324.0317
stuma@spencerfane.com

7018 0360 0000 5330 6897

October 8, 2019

NH Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident

Dear Attorney General Gordon J. MacDonald:

Be advised that the undersigned and this law firm have been retained to represent Hunt Memorial Hospital District, operating as Hunt Regional Healthcare ("Hunt Regional") in connection with the data security incident described below. Hunt Regional is located at 4215 Joe Ramsey Boulevard, Greenville, TX 75401 and provides healthcare in Northeast Texas.

On May 14, 2019, Hunt Regional was notified by law enforcement that it was a victim of a criminal cyber attack in May of 2018 during which sophisticated hackers gained access to the protected health information ("PHI") of approximately 3,740 patients in its network. At that time, Hunt Regional suspected only the patients named by law enforcement were affected by the attack (none of which were residents of your state) and sent notification letters to all those individuals whose information Hunt suspected had been compromised.

Following the discovery of this incident, Hunt Regional engaged independent cyber forensics experts to analyze its systems and the impact of the unauthorized access. During the investigation, Hunt Regional determined on August 14, 2019, that it could not rule out the possibility that the PHI of additional individuals may have also been compromised in the attack. Accordingly, Hunt Regional is sending this notice to your office and the enclosed breach notification letter to residents of your state affected by this incident. Because the hackers gained access to Hunt Regional's network, the hackers were potentially able to access patient medical records which contain sensitive information including patient names, telephone numbers, Social Security numbers, dates of birth, race, and religious preferences. Hunt Regional will notify 21 affected New Hampshire residents of this incident.

Hunt Regional is currently working with the cyber forensics experts to help prevent future unauthorized access in coordination with ongoing vulnerability and penetration testing; and will continue to exercise vigilance to help safeguard personal data in its custody.

Specifically, Hunt Regional has:

- changed or disabled passwords for administrator domain accounts on all servers;

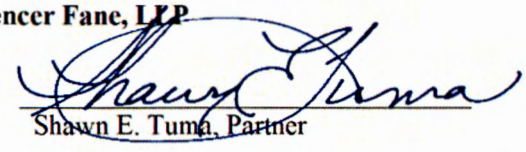
SpencerFane

- increased its Active Directory auditing process in an effort to hold privileged and non-privileged accounts accountable;
- directly enabled policies to ensure accounts with a certain time of inactivity are disabled and subsequently deleted;
- disabled incoming foreign traffic through Hunt Regional's firewall;
- disabled traffic using an anonymous proxy;
- completed a "best practice analysis" on its firewall and implemented tighter security policies to each rule; and
- implemented more robust email security with an inbound security spam, virus, phishing, and email spoof filters.

Hunt Regional provided notification to affected individuals on October 7, 2019, and has partnered with ID Experts, to make available at no cost to affected individuals for twelve months its MyIDCare identity theft protection solution.

A sample copy of the notice sent to the New Hampshire residents is enclosed.

Respectfully,
Spencer Fane, LLP

By: 
Shawn E. Tuma, Partner

Enclosures:
Notice of Data Breach

Hunt Regional Medical Center

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ

BREAK

SEQ
CODE 2D
Ver1G

To Enroll, Please Call:
833-297-6403
Or Visit:
https://ide.myidcare.com/huntmemorialhospital
Enrollment Code: <<XXXXXXXX>>

October 7, 2019

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

On August 14, 2019, Hunt Memorial Hospital District ("HMHD") determined that your personal information may have been compromised in a cyber attack against Hunt Regional Medical Center ("Hunt"). We initially learned on May 14, 2019, that the information of a small number of our patients was compromised in the targeted cyber attack dating back to May of 2018. During the attack, hackers gained access to patient personal information in what we believed at the time to be a limited area of our network. Our investigation up to that point indicated only a subset of our patients, which did not include you, were affected by this incident. We engaged independent cyber forensics experts to analyze our systems and investigate the full impact of the unauthorized access. During this investigation, we determined that your information also was accessible. Out of an abundance of caution we are notifying all patients whose information may have been impacted. We deeply regret that this has occurred and apologize for any inconvenience or concern caused by this incident.

What Information Was Involved

Because the hackers gained access to our network, they were potentially able to access your medical record which contains sensitive information including your name, telephone number, Social Security number, date of birth, race, and religious preference.

What We Are Doing

We are cooperating with the FBI in its investigation of this incident. We have also retained the services of cyber security professionals to further investigate the incident and based on their review, we believe the hackers are no longer in our computer system. In addition, we have reinforced security protocols, increased employee training, enhanced threat detection and monitoring capabilities and will be implementing additional safeguards to strengthen data security within our computer environment.

To assist you in protecting your personal information, we are offering you identity protection services through ID Experts®, the data breach and recovery services expert, including MyIDCare™. MyIDCare services: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 833-297-6403 or going to https://ide.myidcare.com/huntmemorialhospital and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is January 7, 2020.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online, so please do not discard this letter.

We value your privacy and sincerely regret any inconvenience this matter may cause. Our relationship with you, your confidence in our ability to safeguard your personal information, and your peace of mind are very important to us. If you have further questions or concerns, please call 833-297-6403 or go to https://ide.myidcare.com/huntmemorialhospital for assistance.

Sincerely,

Richard Carter, CEO
(Enclosure)

MyIDCare

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://ide.myidcare.com/huntmemorialhospital 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 MyIDCare 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, MyIDCare will be able to assist you.

3. **Telephone.** Contact MyIDCare at 833-297-6403 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

4. **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 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.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

5. **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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	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.

SEQ
CODE 2D

6. 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.

7. 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, at https://www.identitytheft.gov/.

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

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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, 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/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.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, 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/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.