

STATE OF NH  
DEPT OF JUSTICE

2017 MAR 13 AM 8:53

**BakerHostetler**

**Baker & Hostetler LLP**

811 Main Street  
Suite 1100  
Houston, TX 77002-6111

T 713.751.1600  
F 713.751.1717  
www.bakerlaw.com

Lynn Sessions  
direct dial: 713.646.1352  
lsessions@bakerlaw.com

March 10, 2017

**VIA OVERNIGHT DELIVERY**

Attorney General Joseph Foster  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Dear Attorney General Foster:

On January 11, 2017, our client, HealthTexas Provider Network ("HTPN"), which includes Denton Heart Group (the "Clinic"), learned that an external computer hard drive was stolen from the Clinic on or about December 29, 2016. The external computer hard drive was used by the Clinic to back-up or store patient information from the Clinic's electronic health record system and was secured in a locked closet within the Clinic. HTPN promptly reported the theft to law enforcement authorities and is working with law enforcement in its investigation.

The health information contained on the external hard drive concerned Clinic patients and guarantors. It may have included certain demographic information (such as name, date of birth, address and phone number), medical record number, clinic account number, insurance provider's name, insurance group and/or policy numbers, physician's name and clinical information (including diagnosis/conditions, lab test results and medications) related to medical care received at the Clinic between 2009 and 2016. For some individuals, Social Security numbers and/or driver's license numbers were affected.

To help patients and guarantors detect possible misuse of their information, the Clinic is notifying affected individuals and offering those eligible individuals a complimentary one-year membership in credit monitoring and identity theft protection services from Experian. The Clinic has also established a dedicated call center to assist individuals with any questions they may have.

Necessary corrective actions have been taken to safeguard against similar incidents in the future, and HTPN is taking steps to re-evaluate the security of computer devices within its clinics to further protect its patients' information.

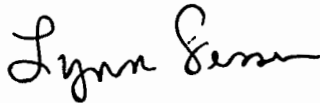
Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

The Clinic is notifying one (1) New Hampshire resident in substantially the same form as the letter attached hereto commencing today, March 10, 2017.<sup>1</sup> As a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Clinic is required to maintain procedures for responding to a breach of security, and notification to the New Hampshire resident is being provided in compliance with these procedures. See N.H. REV. STAT. ANN. § 359-C:20(V); *see also* 45 C.F.R. §§ 160.103 and 164.400 et seq.

Notification is being provided as soon as possible pursuant to the investigation described above, which was necessary to determine the scope of the incident; restore the reasonable integrity of the data system; and identify the individuals potentially affected. See N.H. REV. STAT. ANN. § 359-C:20(I)(a).

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink that reads "Lynn Sessions". The signature is written in a cursive style with a large initial "L".

Lynn Sessions

Enclosure

---

<sup>1</sup> This report is not, and does not constitute, a waiver of personal jurisdiction.



STATE OF NH  
DEPT OF JUSTICE  
2017 JUN 13 11 08:53

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

Protecting the privacy of the personal information of our patients is a critical priority of HealthTexas Provider Network ("HTPN"), which includes Denton Heart Group (the "Clinic"). HTPN is sending you this letter to inform you that portions of your personal health information may have been the subject of a security incident. We want to alert you to the incident, the type(s) of information that may have been included and the actions that HTPN has taken to rectify this matter.

On January 11, 2017, we learned that an external computer hard drive was stolen from the Clinic on or about December 29, 2016. The external computer hard drive was used by the Clinic to back-up or store patient information from the Clinic's electronic health record system and was secured in a locked closet within the Clinic. We promptly reported the theft to law enforcement authorities and we are working with law enforcement in its investigation.

The health information contained on the external hard drive may have included certain demographic information (such as your name, date of birth, address and phone number), <<ClientDef1(driver's license number, Social Security number.)>> medical record number, clinic account number, insurance provider's name, insurance group and/or policy numbers, physician's name and clinical information (including diagnosis/conditions, lab test results and medications) related to medical care you received at the Clinic between 2009 and 2016.

To date, HTPN has no indication that any of the information has been further disclosed or used by any other unauthorized individuals or entities. As a precautionary measure, HTPN recommends that you monitor your credit report to be sure that no suspicious activity has occurred with your personal information. Out of an abundance of caution, we are offering a complimentary one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.** We also recommend that you regularly review the explanation of benefits statements that you receive from your health insurer. If you identify services listed on your explanation of benefits that you did not receive, you should contact your insurance company immediately.

We regret any inconvenience this may have caused you. We take safeguarding patient information seriously and have conducted an internal investigation related to this incident. Necessary corrective actions have been taken to safeguard against similar incidents in the future, and we are taking steps to re-evaluate the security of computer devices within our clinics to further protect our patient's information. Please be assured that the Clinic is committed to providing high quality care and we value the trust you place in us. We hope that you will continue to choose the Clinic for your health care needs.

Should you have any questions or concerns regarding this matter, please do not hesitate to call 1-855-667-7934, Monday to Friday, 8:00 a.m. to 5:00 p.m. Central time.

Sincerely,

Zach Scheele  
Director of Operations

## ACTIVATE PROTECTMYID NOW IN THREE EASY STEPS

1. ENSURE **That You Enroll By: June 13, 2017** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site to enroll: [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem)**
3. PROVIDE **Your Activation Code: <<Member ID>>**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: PC106948

### ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance\*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

**Activate your membership today at [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem)  
or call 877-288-8057 to register with the activation code above.**

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

Even if you choose not to take advantage of the identity theft protection services we are offering, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every 12 months. To order your credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 877-288-8057. Contact information for the three nationwide credit reporting agencies is as follows:

#### **Equifax**

P.O. Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
(800) 685-1111

#### **Experian**

P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
(888) 397-3742

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
(800) 680-7289

\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

**Federal Trade Commission**  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
(877) 438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.