Little River Healthcare Notifies Patients of Data Security Incident

On July 12, 2018, Little River Healthcare (the "Company") became aware of the use of unauthorized transcriptionists by two providers in its Long-Term Care Program. Unbeknownst to the Company, these transcriptionists, or "scribes," were permitted access to the providers' patients' charts, as well as the Company's electronic medical records ("EMR") system. The patient charts contain information such as patient names, dates of birth, medical history, social security numbers, driver's license numbers, and patient home addresses.

As soon as the Company was made aware of the use of these scribes, it instructed the providers to immediately cease all scribing activities and change their EMR passwords, which they did. **At this time the Company has no reason to believe that any patient data was compromised by these scribes in any manner whatsoever.** The two scribes are each trusted family members of the providers at issue and have stated that they did not provide any patient information to any third parties.

However, in compliance with Texas and Federal law, all patients potentially affected by this breach are being notified. Although Little River Healthcare has no reason to believe that patient information is at risk, the Company is taking steps to eliminate or minimize any potential harm that could be caused by the use of these scribes. In an abundance of caution, Little River Healthcare encourages its patients to contact their financial institutions and credit agencies to prevent unauthorized access to personal accounts.

Little River Healthcare has safeguards in place to ensure the privacy and security of all patient health information. Steps are underway to further improve the privacy of its operations and eliminate future risk. The Company is strengthening training for providers regarding the use of third party transcriptionists and the importance of business associate agreements. "Little River Healthcare understands the importance of protecting patient data, and takes this responsibility very seriously," said Jeff Madison, Chief Executive Officer. "With additional training and monitoring, we will enhance safeguards already in place in order to ensure that unauthorized access to patient information does not happen in the future."

Patients may visit Little River Healthcare's website, at www.lrhealthcare.com, for further information, call the company's toll-free number at 833-888-1975 or contact either of the following Little River Healthcare staff:

Kylie Shcherbakov
Associate General Counsel/Chief Compliance Officer
kshcherbakov@lrhealthcare.com

Cheryl Hites
HIM Manager/Privacy Officer
chites@lrhealthcare.com

The following information is provided to help patients or others wanting more information on steps they can take to protect themselves:

What steps can I take to protect my personal information?

- If you detect any suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- Obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- Please notify your financial institution immediately of any unauthorized transactions made or new accounts opened in your name.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your letter.

What should I do to protect myself from payment card/credit card fraud?

We suggest you review your debit and credit card statements carefully for any unusual activity. If you see anything you do not understand or that looks suspicious, you should contact the issuer of the debit or credit card immediately.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is included in the e-mail and letter, and is also listed at the bottom of this page:

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors to possible fraudulent activity within your report and requests that your creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is included in the letter and is also listed at the bottom of this page.

Contact information for the three nationwide credit reporting agencies is as follows:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian Security Freeze
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion (FVAD)
PO Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com