ENT AND ALLERGY CENTER, P.A.

2100 North Green Acres Road, Suite A

Fayetteville, Arkansas 72703

(479) 521-0455

May 31, 2016

**HIPAA Privacy Notification**

**Important Security and Protection Notification**

 At ENT and Allergy Care, P.A., safeguarding our patients’ personal and health information is very important to us -- as we know it is to you. Like many healthcare providers, our office employs the services of a third-party independent contractor for the management and storage of our patient electronic medical records. We believe that such contractors offer significantly greater security for the information contained in these records due to their expertise in the area of electronic and online security. Additionally, the federal government has instituted significant financial penalties for clinics and other health-care providers that do not implement and store medical records electronically. In order to avoid these penalties and to comply with federal rules and regulations, which have recently gone into effect, we began the process of transitioning to electronic medical records in early 2013.

 The vendors that we select to help us better manage and secure our patients’ personal and health information are scrutinized and chosen carefully and must share our commitment to maintaining and preserving the security of your information. With that in mind, security is and must be a paramount priority for our technology vendors. Although security is the top priority, cyber-attacks on information technology and computer files have, unfortunately, become a serious, complicated and recurring event in the world we live in today.

 Our electronic health records contractor, Bizmatics, Inc. (“Bizmatics”), is based in Silicon Valley and has been in the electronic health records market for over 15 years, serving over 15,000 medical professionals and facilitating over 25 million patient interactions. Bizmatics has developed the *PrognoCIS* Electronic Health Record products and services using the latest internet security technology. Like many of our peers, we believe Bizmatics to be the leader in the industry. We selected Bizmatics only after a thorough review process, and they have historically been a good contractor for us.

 Bizmatics recently informed us that a criminal hacker attacked its data servers and gained unauthorized access to Bizmatics customers’ records. This unauthorized access may have compromised the privacy and security of the information contained in those records. Bizmatics believes this unauthorized access began sometime in early 2015 and continued until its discovery in late 2015. Bizmatics has been aggressively proactive in addressing this data attack and in attempting to ascertain what information was accessed by the hackers.

 Bizmatics’ *PrognoCIS* tool fell subject to the attack on Bizmatics’ data servers and, accordingly, Bizmatics’ notified us that we were one of its customers who may have had some of its records accessed by the criminal hacker. The *PrognoCIS* tool stores and organizes our patient files. Accordingly, our records that were potentially compromised could include medical records that we maintain on our patients, such as health visit information, name, address, health insurance information, driver’s license number or other identification information. In these files, a patient’s Social Security number is included although it is believed to be encrypted with only the last four digits being identified. No credit card or financial information is stored in your patient file.

 We were initially notified of the incident by a letter from Bizmatics’ CEO in January 2016. At that time, Bizmatics could not conclude that our patient records were among those that were accessed and had no reason to believe that the data that was compromised had been published or shared in any public manner. Upon becoming aware of the unauthorized access, we began working with Bizmatics, who immediately enlisted law enforcement and a private cybersecurity firm to secure their systems and determine which information had been compromised.

 After further investigation, Bizmatics notified us in early April 2016 that at least some of our electronic patient medical records were potentially accessed and obtained by unauthorized persons. The information contained in the records that may have been accessed included patient names, addresses, health visit information, and at least the last four digits of the patient’s Social Security number. However, the unauthorized access did **not** include credit card number of financial and payment information of our patients, which are maintained on a separate system that is not related to Bizmatics or *PrognoCIS*.

 After conducting various extensive forensic examinations, Bizmatics remains unable to ascertain with any specificity which individual patient records, or which information within specific patient records, was specifically affected. We do not have any information that either confirms or denies that your patient information was accessed or used as a result of this data breach. We also have not received any information indicating that your data was compromised or has been published or shared in any public manner. Nevertheless, because of the risk that our patient information might have been accessed, we believe it is important to provide this notification to you directly and on our website.

 Again, no credit card or financial information was included in your patient file and, at this time, neither we nor Bizmatics have any reason to believe that you have been the victim of identity theft as a result of this unauthorized intrusion. However, we take this incident very seriously, and we are currently in the process of implementing safeguards to protect your information and to answer any questions that you may have by offering twelve months of free credit, fraud and identity-theft monitoring services through Equifax Consumer Services LLC and by creating a toll-free phone dedicated solely to answering questions about this incident. A personal notification letter will be mailed to each affected patient as soon as possible, which is expected to be in the next 5-10 business days, that will provide more information with respect to these services, and we will update this notification on our website once these services have been finalized. Additionally, we recommend that you take the following recommendations regarding preventative steps that may be taken by you to further protect your privacy and security.

 **First**, we recommend that you closely monitor your financial accounts and, if you notice any suspicious or unauthorized activity, promptly contact your financial institution.

 **Second**, we recommend that you closely monitor any Explanation of Benefit forms you receive from your health insurance provider and, if you see any suspicious activity, promptly contact your health insurance provider.

 **Third**, even if you do not feel the need to register for a credit monitoring service, as a precautionary measure, we recommend that you regularly review statements from your bank, credit card, and other accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com,](http://www.annualcreditreport.com/) by calling toll-free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies:

|  |  |  |
| --- | --- | --- |
| **Equifax**P.O. Box 740241 | **Experian**P.O. Box 9532 | **TransUnion**P.O. Box 6790 |
| Atlanta, GA 30374 | Allen, TX 75013 | Fullerton, CA 92834 |
| [www.equifax.com](http://www.equifax.com/) | [www.experian.com](http://www.experian.com/) | [www.transunion.com](http://www.transunion.com/) |
| 1.800.685.1111 | 1.888.397.3742 | 1.800.916.8800 |

When you receive your credit reports, look them over carefully. Look for accounts that you did not open and/or inquiries from creditors that you did not initiate. Also check to see if your personal information on the credit report is accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend that you remain vigilant in your review of your account statements and credit reports. You should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state’s attorney general, and/or the Federal Trade Commission. A copy of a police report may be required by creditors to clear up your records.

 **Fourth**, if you believe you have been the victim of financial identity theft, we recommend calling your local law enforcement and filing a police report. Retain a copy of the report, as many creditors will want the information it contains to absolve identity theft victims of fraudulent activity. We also recommend filing an identity theft complaint with the FTC at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or at (877) 438-4338. Your complaint will be added to the FTC’s Identity Theft Clearinghouse where it will be accessible to law enforcement for use in their investigations. Additionally, consider placing a fraud alert or a security freeze (also called a credit freeze) on your credit file. Security freeze laws vary from state to state. For more information about fraud alerts and security freezes, please see the Federal Trade Commission’s guidance at [http://www.consumer.ftc.gov/articles/0279-extended-fraud-](http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes) [alerts-and-credit-freezes.](http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes)

 **Fifth**, You can minimize the threat of identity theft by improving your password practices. Use different passwords for all your accounts. Make those passwords strong with at least eight characters, including a mix of letters, numbers, and symbols ($%#!\*@). Change your passwords from time to time. For additional guidance on passwords and securing your accounts, see:

[http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/passwords-](http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/passwords-and-securingyour-) [and-securing your-](http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/passwords-and-securingyour-) accounts.

 **Sixth**, Scam artists “phish” for victims by pretending to be banks, stores, government agencies, or other trusted sources. They do this over the phone, by email, and by postal mail. Do not respond to any request to verify your account number or password. Legitimate companies do not request this kind of information in this way. If an email looks suspicious, don’t click on any links in that email.

 We are keenly aware of how important your personal information is to you, and we regret that this situation has occurred. We are providing this notification to comply with applicable law regarding the unauthorized disclosure of your protected health information. The ENT and Allergy Center, P.A. is committed to providing quality care, including protecting your personal information, and we want to assure you that we have the policies and procedures in place to strive to best protect your privacy.

 We want to assure that your questions about this incident are answered so we have arranged to have call center associates available to address your concerns. If you have any questions, please contact our Office Manager, Beverly Hodges at 479-521-0455 or entclinic@arkansas.net. I deeply regret that this incident has occurred, and I hope that it will not negatively affect you or the security of your personal information.

 Very truly yours,

 Stephen Cashman, M.D.

 Stephen Cashman, M.D.,

 President of ENT and Allergy Center, P.A.