Dental Office of Dr. Douglas Boucher, DDS and Dr. Andrea Yaley, DDS

July 10, 2017

Notice of Data Breach
at our Menlo Park Dental Office

Dear Patients of Dr. Douglas Boucher and Dr. Andrea Yaley,

Our office is committed to protecting the security and confidentiality of your personal information. We are writing to inform you about an incident involving some of your information that may have been accessed without authorization. Our office takes this incident very seriously. We want to provide you with information about what happened and help you take steps to protect yourself and your personal information. If you previously received an email from us about a ransomware attack, this is a follow-up notice about the same attack.

What happened?
On June 2, 2017 our office received a ransomware notice from someone who had hacked our computer systems. We believe the hacking occurred on or about May 19, 2017. Upon receiving the notice, we immediately contacted the local and federal authorities, shut down all our computer systems, and implemented additional security measures to preclude further attacks. We were able to restore our health records from our backup systems.

What information was involved?
The hacker did access our email system and may have accessed our patient dental health records. Our email system contains patient email addresses and contact information. Our patient dental health records include our patients' full names and home addresses, dates of birth, Social Security Numbers, dental diagnoses, dental treatment and other personal and health information collected for your dental treatment. We do not know whether the hacker took information from our dental health records, but it is possible that he did so, so we urge you to take the protective measures described below.

What we are doing.
We received the ransomware notice on June 2. We immediately called in security experts, and shut down our computer systems while we installed additional security measures to preclude further attacks. We sent email notices to our patients who are in our email system. We are undertaking a comprehensive assessment of our IT practices and policies and we are actively working with the Menlo Park Police Department, Sheriff Department, and FBI on the case to identify and prosecute the perpetrator. Their investigation has not delayed this notification.

We are committed to helping those people who may have been impacted by this unfortunate situation. That's why we are offering to provide you with access to Triple Bureau Credit

Monitoring* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to any of one of your Experian, Equifax, or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. These services will be provided by CyberScout, a company that specializes in identity theft education and resolution.

How do I enroll for the free services?

To enroll in **Credit Monitoring*** services at no charge, please log on to **https://www.myidmanager.com** and follow the instructions provided. **When prompted please provide the following unique code to receive services:**

Name	**code**	**spouse**	**spouse code**
Adult dep.	**Adult dep code**	**adult dep.2**	**adult dep. Code2**

For guidance with the CyberScout services, or to obtain additional information about these services, **please call the CyberScout help line *1-800-405-6108*** and supply the fraud specialist with your unique code.

What you can do. Here are some steps you can take to help prevent harm in case the person took personal information:

- You can report possible identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system. The automated system allows you to flag your file with a fraud alert at all three bureaus. This helps stop a thief from opening new accounts in your name. The alert stays on for 90 days. Each of the credit bureaus will send you a letter confirming your fraud alert and giving instructions on how to get a copy of your credit report. Each report you receive will contain a telephone number you can call to speak to someone in the credit bureau's fraud department.

  Experian 1-888-397-3742
  experian.com/fraud/center.html

  Equifax 1-888-766-0008
  alerts.equifax.com

  TransUnion 1-800-680-7289
  transunion.com

  When you receive your credit reports, read them carefully. Look for accounts you don't recognize. Look in the inquiries section for names of creditors from whom you haven't requested credit. If you find anything you don't understand, call the credit bureau at the telephone number listed on the report.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection and in order to confirm your identity.

- Consider a credit freeze. The strongest protection against new accounts being opened in your name is a credit freeze, also called a security freeze. A freeze means that your file cannot be shared with potential creditors, insurers, employers, or residential landlords without your permission. You can find out how to freeze your credit by calling one of the toll-free numbers or going to one of the web sites listed above.

- You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

Other Important Information.
If someone you don't know calls you and asks for personal or financial information, don't provide it until you are certain that the request is proper. If you are uncertain, take a telephone number and call back when you have had a chance to investigate the request.

Be careful responding to emails that appear to come from our office. We believe the hacker has sent emails to some of our patients using fake email addresses, such as andreayaley@excite.com. This is a fake account. Dr. Yaley's email address is dryaleydds@gmail.com. **Don't provide personal or financial information or passwords in response to an email – we will never ask you for these in an email.**

As you may be aware, ransomware attacks on businesses, government entities (including the U.S. Department of Defense), healthcare providers, education institutions, and individuals are increasing at an unpresented pace, worldwide. We are truly thankful for our patients, the Menlo Park community, our business partners, and law enforcement who have rallied around us to help us continue to do the work we love, and we want to express our deepest regret for this incident that has impacted all of us. Our team is looking forward seeing you at your next appointment as we continue our mission to provide you with excellent dental services. Please feel free to contact us anytime with any questions you may have.

For More Information, please call our office at (650) 325-8030 or via email at dryaleydds@gmail.com. You may also visit douglasboucherdds.com or write to 825 Oak Grove Ave #401 Menlo Park, CA 94025.

Yours sincerely,

Dr. Andrea Yaley, DDS