VIA U.S. MAIL

Washington State Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notice of Breach in the Security of Protected Health Information

To Whom It May Concern:

I represent Zachary E. Adkins DDS ("the Company"), which is a New Mexico-based dental practice. Pursuant to RCW § 19.255.010(10), enclosed is a copy of an electronic breach notification submitted with the U.S. Office for Civil Rights at the Department of Health and Human Services regarding a breach in the security of protected health information, which affected residents of the state of Washington.

I believe this provides you with all information necessary for your purposes and to comply with Washington law. However, if you have any questions or need further information, please contact me.

Very truly yours,

FREEMAN MATHIS & GARY, LLP

David A. Cole

DAC/kam
Enclosure
3238163_1
Breach Tracking Number: Q4K355LGR8

Thank you for filing a breach notification via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your breach notification. Your breach notification will be assigned to an OCR staff member for review and appropriate action. If OCR has any questions about the breach notification you submitted, we will contact you directly. Otherwise, you will receive a written response indicating whether or not OCR has accepted your breach notification for investigation.

Please do not fax, email, or mail a copy of this breach notification to us as that may delay the processing of your breach notification.

If you have any additional information to add to your breach notification, you may call 1-800-368-1019. Please reference the number given by OCR when submitting your breach notification.

* Breach Affecting: 500 or More Individuals
* Report Type: Initial Breach Report

* Are you a Covered Entity filing on behalf of your organization? Yes

**Covered Entity**

* Name of Covered Entity: Zachary E. Adkins, DDS
* Type of Covered Entity: Healthcare Provider
* Street Address Line 1: 3900 Eubank Blvd. NE
  Street Address Line 2: Ste. N17
* City: Albuquerque
* State: New Mexico
* ZIP: 87111

**Covered Entity Point of Contact Information**

* First Name: David
* Last Name: Cole
* Email: dcole@fmglaw.com
* Phone Number: (Include area code): (770) 818-1287 Work

* Breach Start Date: 11/30/2017 * Breach End Date: 11/30/2017
* Discovery Start Date: 11/30/2017 * Discovery End Date: 11/30/2017
* Approximate Number of Individuals Affected by the Breach: 3677

* Type of Breach: Theft

* Location of Breach: Other Portable Electronic Device

* Type of Protected Health Information Involved in Breach: Clinical Demographic
On November 30, 2017, a laptop bag containing an external hard drive from Dr. Adkins' office was stolen. The hard drive contained backup files from two programs used in his office – Florida Probe and Dentrix. The files in the Florida Probe backup were unencrypted, but contained only limited information of patient names and corresponding teeth pocket depth measurements that are used for periodontal exams. The files in the Dentrix backup contained patient names, addresses, phone numbers, dates of birth, Social Security numbers, treatment information, and insurance information. The Dentrix backup is protected within the software through Dentrix's data-masking techniques that use cryptographic technology. It would be accessible only to someone who had the Dentrix software along with Dr. Adkins' office's unique software serial number and his Dentrix username and password.

Privacy Rule Safeguards (Training, Policies and Procedures, etc.)
Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)
Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

* Individual Notice Provided
  Provided Start Date: 01/25/2018
  Projected/Expected End Date: 01/25/2018

Was Substitute Notice Required? Yes

Was Media Notice Required? Yes

* Select State(s) and/or Territories in which media notice was provided:
  New Mexico

Changed password/strengthened password requirements
Implemented new technical safeguards
Improved physical security
Provided individuals with free credit monitoring
Revised policies and procedures
Took steps to mitigate harm
Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

* Name: Kacie Manisco   Date: 01/25/2018
Dear <<First Name>>, 

Thank you for allowing me, Zachary E. Adkins, DDS to be your dentist. My team and I take great pride in providing excellent quality dentistry with integrity and compassion. Our patients come first. We take patient privacy very seriously, and I am writing to notify you of a recent incident that involved your information. 

On November 30, 2017, a laptop bag containing an external hard drive from our office was stolen. The hard drive contained backup files from two programs used in our office – Florida Probe and Dentrix. The files in the Florida Probe backup were unencrypted, but contained only limited information, including patient names and corresponding teeth pocket depth measurements that we use for periodontal exams. The files in the Dentrix backup contained patient names, addresses, phone numbers, dates of birth, Social Security numbers, treatment information, and insurance information. Fortunately, the Dentrix backup is protected by a data-masking technique using cryptographic technology. It would be accessible only to someone who had the Dentrix software along with our office’s unique software serial number and our Dentrix username and password. Moreover, no financial information, bank account information or credit card numbers are ever kept on file and this information has not been compromised as a result. 

Based on this, we believe it is unlikely that any person who acquired the hard drive would be able to access the files in the Dentrix backup, or that the files in the Florida Probe backup could be used by anyone to cause any harm to you. But because we have not been able to recover the hard drive since it was stolen, we do not know what has become of it and cannot confirm with certainty whether anyone has actually accessed or viewed any of the files on it. Therefore, we have chosen to notify all of our patients about this issue out of an abundance of caution because we understand how important your personal information is to you. 

Please know that we take the protection of your personal information seriously and we are taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent future incidents. We promptly reported the theft to law enforcement and will continue to cooperate with any investigation. We are also reviewing our policies and procedures and taking steps to further strengthen the security of our patients’ information, including transitioning our backup to a cloud-based service. 

As an added precaution to help protect your information from potential misuse, we are offering identity theft protection services through ID Experts® and its MyIDCare™ solution at no cost to you. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.
We strongly encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 800-310-0268 or going to www.idexpertscorp.com/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Mountain Time. Please note the deadline to enroll is April 26, 2018. Please refer to the enclosed documentation for further instructions from ID Experts® on how to enroll in MyIDCare™, and for additional information on steps you may take to help protect your information from misuse.

We are very sorry for any concern or inconvenience this incident has caused or may cause you. If you have any other questions or concerns that you would like to discuss, please call our dedicated, toll-free incident response hotline at 800-310-0268 or go to www.idexpertscorp.com/protect.

Sincerely,

Zachary Adkins, D.D.S.
**Recommended Steps to Help Protect Your Information**

Please Note: Minors, under the age of 18, should not have a credit history established and are under the age to secure credit. Therefore credit monitoring may not be applicable at this time. All other services provided in the membership will apply. No one is allowed to place a fraud alert on your credit report except you, please follow the instructions below to place the alert.

1. **Website and Enrollment.** Go [www.idexpertscorp.com/protect](http://www.idexpertscorp.com/protect) and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive MyIDCare Member Website where you will find other valuable educational information.

2. **Activate the credit monitoring** provided as part of your MyIDCare membership. Credit and CyberScan monitoring are included in the membership, but you must personally activate it for it 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 800-310-0268 to gain additional information about this incident and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. **Review personal account statements and credit reports.** We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. 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](http://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 visiting their Member website and filing a theft report. Otherwise, you should report any incorrect information on your report to the credit reporting agency.

   If you file a theft report with MyIDCare, 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.

5. **Report suspected fraud.** 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 should report suspected incidents of identity theft to local law enforcement, your state’s Attorney General, and/or the Federal Trade Commission.

6. **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:

   - **Equifax Fraud Reporting**
     1-866-349-5191
     P.O. Box 105069
     Atlanta, GA 30348
     [www.alerts.equifax.com](http://www.alerts.equifax.com)

   - **Experian Fraud Reporting**
     1-888-397-3742
     P.O. Box 9554
     Allen, TX 75013
     [www.experian.com](http://www.experian.com)

   - **TransUnion Fraud Reporting**
     1-800-680-7289
     P.O. Box 2000
     Chester, PA 19022
     [www.transunion.com](http://www.transunion.com)
It is only necessary to contact 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.

7. **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 in writing 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. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to $5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

8. **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.

- **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
- **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, (888) 743-0023.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, (877) 877-9392.
- **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400.

9. **Summary of Rights Under the Fair Credit Reporting Act.** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. You have certain rights under the FCRA, including: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (your “file disclosure”); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (8) You may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (9) You may seek damages from violators; and (10) Identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit. States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.