NOTIFICATION OF
DATA SECURITY INCIDENT

Point of Contact	**Dated**:09/18/2019 **Submitted by:** Kevin Scott **Title**: Attorney **Firm Name** (if other than entity): Bryan Cave Leighton Paisner LLP **Telephone**: (312) 602-5074 **Email**: kevin.scott@bclplaw.com **Relationship to Entity whose information was compromised**: Counsel

Impacted Organization	**Name and address of Entity that owns or licenses the data that was subject to the breach**: Name: Wood Ranch Medical Street Address: 135 Macaw Ln, Ste 210 City: Simi Valley State: California Zip Code: 93065 Country: United States of America

Overview of Incident	**General Description of Security Incident:** On August 10, 2019, Wood Ranch Medical ("WRM") suffered a ransomware attack on its computer systems. The attack encrypted WRM's servers, containing patient electronic health records as well as its backup hard drives. The electronic healthcare records include patient names, addresses, dates of birth, medical insurance and related health information. **Steps Taken by Organization to Address Incident:** Unfortunately, the damage to WRM's computer system was such that WRM is unable to recover the data stored there and, with its backup system encrypted as well, WRM cannot rebuild its medical records. WRM will be closing its practice and ceasing operations on December 17, 2019. Between now and December 17, 2019, WRM will assist its patients in transitioning to other healthcare providers.

Industry	[] Governmental Entity []Other Governmental Entity [] Educational [**X**] Health Care [] Financial Services []Not-for-profit []POS Vendor []General Business []Insurance [**]**Retail/Merchant []Utility []Other Commercial [] Other

Type of Incident	[]Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape) [] Internal system breach [] Insider wrongdoing [**X**] External system breach (e.g., hacking) []Inadvertent disclosure [] Payment card fraud []Improper disposal []Phishing []Theft []Other:

Data Potentially Impacted	**Information Acquired: Name or other personal identifier in combination with** (please select all that apply): [**X**]Name []Social Security Number []Driver's license number or non-driver identification card number []Federal identification card number []Passport Number []Individual taxpayer ID number []Credit card number []Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account []Biometric information []DNA [**X**] Medical information [**X**]Diagnosis of mental/physical condition by healthcare professional [**X**] Insurance information [] Other:

Data Subjects	**Have impacted residents of the state been notified?** [**X**] Yes [] No **Manner of Notification to Affected Persons** [**X**] Written [] Electronic [] Telephone [**X**] Substitute notice **Identify Theft Protection Service Offered:** []Yes [**X**]No **Credit Monitoring Service Offered:** []Yes [**X**] No

An example of the notification letter template is attached to this notice.

Wood Ranch Medical
Dr. Shayla Kasel
Family Physician

September 18, 2019

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident that may have affected some of your personal healthcare information. We take the protection of our patients' information seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter provides you with information about what happened.

What happened?

On August 10, 2019, we suffered a ransomware attack on Wood Ranch Medical's computer systems. Ransomware is a computer virus that encrypts our computer system until and unless we pay money (i.e., the ransom) demanded by the attackers. The attack encrypted our servers, containing your electronic health records as well as our backup hard drives. These rampant attacks continue to challenge everyone in the business and medical communities. We believe it is likely the attacker only wanted money and not the information on our computers.

What information was involved?

While we have no reason to believe that your healthcare information was taken, the encrypted system contained your electronic healthcare records which include your name, address, date of birth, medical insurance and related health information.

What we are doing.

We discovered the attack almost immediately and began working to restore our systems. Unfortunately, the damage to our computer system was such that we are unable to recover the data stored there and, with our backup system encrypted as well, we cannot rebuild our medical records. We will be closing our practice and ceasing operations on December 17, 2019. As much as I have enjoyed providing medical care to you, I will not be able to attend to you professionally after that date. Between now and December 17th, we will work with you as you seek another medical practitioner for you and your family's healthcare needs. If you require an appointment for medication refills you must contact our office at (805) 306-0222 as soon as possible prior to December 17th.

What you can do.

Although we have no reports of misuse of your or anyone's information, we recommend that you review the additional information enclosed, which contains important steps you can take to further protect your personal information.

For more information.

If you have any questions, please call 1-833-943-1375, Monday through Friday from 6:00 am - 3:30 pm Pacific Time. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

A. Kasel M.D.

Shayla Kasel, MD

Additional Important Information

For residents of Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Virginia, and Vermont: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.
For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.
For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of Illinois, Maryland, North Carolina, and Rhode Island:

You can obtain information from the Maryland, North Carolina, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General	**Rhode Island Office of the Attorney General**	**North Carolina Office of the Attorney General**	**Federal Trade Commission**
Consumer Protection Division	Consumer Protection	Consumer Protection Division	Consumer Response Center
200 St. Paul Place	150 South Main Street	9001 Mail Service Center	600 Pennsylvania Ave, NW
Baltimore, MD 21202	Providence RI 02903	Raleigh, NC 27699-9001	Washington, DC 20580
1-888-743-0023	1-401-274-4400	1-877-566-7226	1-877-IDTHEFT (438-4338)
www.oag.state.md.us	www.riag.ri.gov	www.ncdoj.com	www.identitytheft.gov

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (https://www.experian.com/fraud/center.html) or TransUnion (https://www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9544	Chester, PA 19014-0200
www.equifax.com/personal/credit-report-services/	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.