MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: 267-930-4784
Fax: 267-930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 16, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Gordon MacDonald:

We represent Centrelake Medical Group, Inc. ("Centrelake"), 3115 E. Guasti Road, Ontario, California 91761, and are writing to notify your office of an incident that may affect the security of protected health information relating to six (6) New Hampshire residents. The investigation into this incident is ongoing, and this notice may be supplemented with any substantive information learned after submission of this notice. By providing this notice, Centrelake does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 19, 2019, Centrelake discovered that certain computers and servers had been infected with a virus that prohibited access to patient files. The integrity of the information system was immediately restored and an investigation was launched with the assistance of a forensic expert, to determine the capabilities of the virus and how it was introduced to the system. As part of the extensive investigation, it was determined that this virus was introduced by an unknown third-party that had access to certain servers on Centrelake's information system which contain personal and protected health information relating to current and former Centrelake patients. After a review of available forensic evidence, it was determined that the suspicious activity began on the network on January 9, 2019, lasting until the virus infection on February 19, 2019.

Notice to New Hampshire Residents

While the investigation is ongoing, and there is currently no evidence the unknown third-party viewed or took information stored on the impacted servers, it has been confirmed that the servers housed files and software applications containing information which may include patients' names, addresses, phone numbers, Social

Security numbers, services performed and diagnosis information, driver's license information, health insurance information, referring provider information, medical record number and dates of service. The types of personal information may vary by individual. Centrelake determined that the protected health information relating to six (6) New Hampshire residents may have been stored on the server. On April 16, 2019, Centrelake issued a press release regarding this incident to media serving California. Centrelake also conspicuously posted notice of this incident on the homepage of its website, where it will remain for ninety days. The press release and posting on Centrelake's website are provided in substantially the same form as what is attached hereto as ***Exhibit A***. Additionally, beginning on or about April 16, 2019, Centrelake is providing written notice of this incident to business partners and potentially impacted individuals as required by relevant regulation. Notice is being provided to potentially impacted patients of Centrelake in substantially the same form as the letter attached hereto as ***Exhibit B***.

Other Steps Taken and To Be Taken

Centrelake is providing potentially impacted individuals access to 1 free year of identity monitoring and restoration services through Kroll and has established a dedicated hotline for individuals to contact with questions or concerns regarding this incident. Additionally, Centrelake is providing potentially impacted individuals with helpful information on how to protect against identity theft and fraud, including how to place a fraud alert and security freeze on one's credit file, the contact information for the national consumer reporting agencies, how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, state attorney general, and law enforcement to report attempted or actual identity theft and fraud. Centrelake is also providing written notice of this incident to the Department of Health and Human Services, the Centers for Medicaid and Medicare Services, as well as consumer reporting agencies and other state regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4784.

Very truly yours,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/ajd

EXHIBIT A

CENTRELAKE
IMAGING & ONCOLOGY

CENTRELAKE MEDICAL GROUP, INC. PROVIDES NOTICE OF DATA INCIDENT

Ontario, California – April 16, 2019 – Centrelake Medical Group, Inc. ("Centrelake") is taking action after it recently became aware that there was an incident in which an unknown third party may have gained access to the data in its practice. Although there is no indication of actual or attempted misuse of patient information, Centrelake is notifying patients whose records may have been subject to unauthorized access and providing these patients with information and resources that can be used to better protect against the possibility of identity theft or fraud if they feel it is appropriate to do so.

Centrelake takes this incident, and patient privacy, very seriously, and is taking steps to help prevent another incident of this kind from happening by continuing to review its processes, policies, and procedures that address data privacy.

To better assist those who may potentially have been affected by this event, Centrelake has established a toll-free privacy line staffed with individuals familiar with this incident and how to better protect against the possibility of identity theft and fraud, and you can direct all questions and concerns to this line by calling 1-866-736-0792 between 8:00 a.m. and 5:30 p.m. PST, Monday through Friday, excluding major holidays.

What Happened

On February 19, 2019, Centrelake discovered its information system had been infected with a virus that prohibited its access to its files. Centrelake immediately worked to restore its information system and launched an investigation, with the assistance of third-party forensics, to determine the nature and scope of the incident. As part of Centrelake's ongoing investigation, it determined this virus was introduced by an unknown third-party that had access to certain servers on its information system which contain personal and protected health information relating to current and former Centrelake patients. After a review of available forensic evidence, Centrelake determined that suspicious activity began on its network on January 9, 2019, lasting until the virus infection on February 19, 2019.

Information Affected

While the investigation is ongoing, and there is no evidence the unknown third-party viewed or took patient information stored on the systems, it has been confirmed that the impacted servers housed files and software applications containing information which may include patients' names, addresses, phone numbers, Social Security numbers, services performed and diagnosis information, driver's license information, health

insurance information, referring provider information, medical record number, and dates of service.

Notification

Centrelake is providing notification to impacted patients and business partners and providing notification to required regulators about this incident.

Fraud Prevention Tips

Centrelake encourages affected individuals to remain vigilant against incidents of identity theft and fraud and to seek to protect against possible identity theft or other financial loss by regularly reviewing their financial account statements, credit reports, and explanations of benefits for suspicious activity. Anyone with questions regarding how to best protect themselves from potential harm resulting from this incident, including how to receive a free copy of one's credit report, and place a fraud alert or security freeze on one's credit file, is encouraged to call 1-866-736-0792 between 8:00 a.m. and 5:30 p.m. PST, Monday through Friday, excluding major holidays.

###

EXHIBIT B

CENTRELAKE
IMAGING & ONCOLOGY

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

Centrelake Medical Group, Inc. ("Centrelake") writes to inform you of a recent event that may affect the security of some of your personal information. While we are unaware of any actual or attempted misuse of your personal information, out of an abundance of caution, we are providing you with information about the incident, steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened? On February 19, 2019, we discovered our information system had been infected with a virus that prohibited our access to our files. We immediately worked to restore our information system and launched an investigation, with the assistance of third-party forensics, to determine the nature and scope of the incident. As part of our ongoing investigation, we determined this virus was introduced by an unknown third-party that had access to certain servers on our information system which contain personal and protected health information relating to current and former Centrelake patients. After a review of available forensic evidence, we determined that suspicious activity began on our network on January 9, 2019, lasting until the virus infection on February 19, 2019.

What Information Was Involved? While our investigation is ongoing, we have no evidence the unknown third-party accessed or acquired protected information stored on the servers. Nevertheless, we confirmed these servers housed files and software applications containing information relating to you, which may include your name, address, phone number, Social Security number, services performed and diagnosis information, driver's license information, health insurance information, referring provider information, medical record number, and dates of service. While the types of personal information may vary by individual, out of an abundance of caution, we are providing notice of this incident to you given we cannot rule out unauthorized access to this information occurred.

What is Centrelake Doing? We take this matter, and the security and privacy of our patients' information, very seriously. In addition to launching the ongoing investigation and restoring the integrity of our information system, we are reviewing our policies and procedures and enhancing the security of our information system to mitigate the risk an incident like this will occur in the future. We are also providing you notice of this incident, as well as complimentary access to identity monitoring services and information on what you can do to better protect against the possibility of identity theft and fraud.

What Can You Do? While we have no evidence your information was subject to unauthorized access, or that your information has been or will be misused, you can take steps to better protect against the possibility of identity theft and fraud by enrolling to receive the complimentary credit monitoring and identity theft restoration services we are offering. You can also review the additional information on protecting against misuse of your information. This additional information, as well as instructions on how to enroll and receive the complimentary monitoring and restoration services, are included in the attached Privacy Safeguards.

For More Information. We understand you may have questions relating to this event and this letter. We have established a privacy line staffed with individuals familiar with this incident and how to better protect against the possibility of identity theft and fraud, and you can direct all questions and concerns to this line by calling 1-866-736-0792, Monday through Friday, 8 a.m. to 5:30 p.m. Pacific Time. You may also write to: Centrelake Medical Group Inc., 3115 E. Guasti Road, Ontario, CA 91761.

We apologize for any inconvenience this incident may cause you and remain committed to the privacy and security of our patients' information.

Sincerely,

Shan Niroola
Centrelake Medical Group, Inc.

PRIVACY SAFEGUARDS

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **July 17, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-866-736-0792. Additional information describing your services is included with this letter.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.