[INSERT DATE]

[INSERT NAME]
[INSERT ADDRESS]

Re: Notification to American Anesthesiology Patients of Business Associate Data Security Event

Dear [NAME],

American Anesthesiology, Inc. and its affiliated anesthesia practices ("American Anesthesiology") are notifying their patients of a security event at one of their service providers that may have impacted patients' personal information.

MEDNAX Services, Inc., a service provider and business associate of American Anesthesiology (the "business associate"), has reported to American Anesthesiology that patients' personal information was stored within email accounts that were accessed by an unauthorized party following a phishing event.

American Anesthesiology is not aware of any actual or attempted misuse of personal information as a result of this event. However, we take patient privacy very seriously, and want to make sure you are aware of the facts surrounding this event so that you can take the appropriate precautions you feel are needed to protect your personal information. We have enclosed information on several identity protection resources, including a complimentary subscription to credit monitoring.

What Happened?

On July 16, 2020, American Anesthesiology was notified that an unauthorized party had gained access to several email accounts on our business associate's Microsoft Office 365 hosted email system ("O365 System") between June 17, 2020 and June 22, 2020 through phishing. "Phishing" occurs when an email is sent that looks like it is from a trustworthy source, but it is not. The phishing email prompts the recipient to share or give access to certain information to an unauthorized party.

Based on the investigation that our business associate performed, and ultimately completed in November 2020, your personal information was stored within one or more of these email accounts. We cannot tell from available forensic evidence if these files were actually viewed by the unauthorized party. The unauthorized actions we are able to see in these email accounts all appear to be in furtherance of unsuccessful payroll fraud attempts. Efforts to change the bank details for employee pay were not successful.

What Information Was Available?

Our business associate has reported that personal information may have included: (1) patient contact information (such as patient name, guarantor name, address, email address, and date of birth); (2) state identification number and/or social security number; (3) health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number); (4) medical and/or

treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (5) billing, payment, and claims information (invoices, payment details, submitted claims and appeals, and patient account identifiers used by your provider). Please note that not all of these data fields may have been involved for all individuals.

What We Are Doing

After discovering the phishing event, our business associate took steps to terminate the unauthorized party's access to the O365 System. This included, for example, resetting each user's password for the email accounts where unauthorized activity was detected. The email accounts on the O365 system that were used by American Anesthesiology employees have now been moved over to our email system. We have added authentication requirements to restrict access to the email accounts of these American Anesthesiology employees. We also will be introducing additional authentication and security training requirements for all of our employees in 2021 to counteract phishing and other social engineering techniques.

What You Can Do

In addition to enrolling in complimentary credit monitoring, the enclosed Reference Guide includes information on general steps you can take to monitor and protect your personal information. We encourage you to carefully review credit reports, patient billing statements, and statements sent from your insurance company to ensure that all account activity is valid; any questionable charges should be promptly reported.

For More Information

If you have any questions or would like additional information, please refer to the enclosed Reference Guide, visit www.AmericanAnesthesiology.kroll.com, or call toll-free 1-833-971-3306. This call center is open Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

We regret that this event occurred and are very sorry for any inconvenience this event may cause you.

Sincerely,

Gail Madison-Brown
Vice President for Compliance

IDENTITY PROTECTION REFERENCE GUIDE

1. Review your Credit Reports. We recommend that you remain vigilant by monitoring your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts with the three credit bureaus. 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. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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 should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security 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.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

4. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements, medical provider statements, and insurance statements for fraudulent activity and report anything suspicious to the respective institution or provider.

5. You can obtain additional information about the steps you can take to avoid identity theft and more information about fraud alerts and security freezes from the Federal Trade Commission (FTC). You may contact the FTC, Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

***

District of Columbia Residents: You can obtain additional information about identity theft prevention and protection from the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, https://oag.dc.gov.

Maryland Residents: You can obtain additional information about identity theft prevention and protection from the Maryland Attorney General, Identity Theft Unit at: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, 1-888-743-0023 or (410) 576-6491, https://www.marylandattorneygeneral.gov.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

American Anesthesiology, Inc. is offering you a one-year, complimentary membership for IdentityWorks[SM], a product offered by Experian®, to help with detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: **<<insert>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **<<insert>>**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.288.8057 by **<<insert>>.** Be prepared to provide engagement number **<<insert>>** as proof of eligibility for the identity restoration services by Experian.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.288.8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.