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

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

RE: NOTICE OF DATA EVENT

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

Advanced Medical Practice Management ("AMPM") is a third-party medical billing administrator that provides billing services to certain healthcare providers, including <<b2b_text_1 (Covered Entity)>>. AMPM is writing on behalf of <<b2b_text_1 (Covered Entity)>>, to notify you of a recent event at AMPM that may have affected the privacy of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so.

What Happened? On August 5, 2021, AMPM discovered suspicious activity associated with certain files within our environment. AMPM quickly took steps to secure the network, and began an investigation to determine the nature and scope of the activity. Our investigation subsequently determined that an unauthorized actor acquired certain files from our environment between July 11, 2021 and July 13, 2021. Given that these certain files were accessed without authorization, we then began a comprehensive review of the files to determine the information potentially impacted by this incident and to whom the information related for purposes of notification. Upon completion of this review, we then worked diligently to reconcile this information with our internal records to confirm the individuals whose information may have been affected and the appropriate contact information for those individuals. We completed this review on January 27, 2022, and thereafter worked to provide notification to organizations whose patients were potentially impacted, including <<b2b_text_1 (Covered Entity)>>, in order to obtain necessary information and approval, and thereafter began notifying potentially impacted individuals as quickly as possible. We are notifying you out of an abundance of caution because your information was determined to be present in one of the specific files involved, and therefore may have been accessed during this incident.

What Information Was Involved? Our investigation determined that the impacted information may include your <<b2b_text_2 ("name" and Data Elements)>>. While we have no evidence of any actual or attempted misuse of your information, we are letting you know out of an abundance of caution and providing information and resources to assist you in helping to protect your personal information, should you feel it appropriate to do so.

What We Are Doing. AMPM treats its responsibility to safeguard information in its possession as an utmost priority. As such, we responded quickly to this event and have been working diligently to provide you with an accurate and complete notice of the incident. Our response to this event also included prompt reporting to federal law enforcement. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and enhancing our existing policies and procedures relating to data protection and security. We have also instituted additional security measures, as well as provided additional training to employees, to mitigate any risk associated with this incident and to better protect against future incidents. We are also notifying relevant state and federal regulators, as required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and monitoring your free credit reports for suspicious activity and to detect errors. Further, please review the enclosed "*Steps You Can Take to Help Protect Personal Information*" section of the letter for additional information.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our dedicated call center at [XXX-XXX-XXXX], which is available from 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding some U.S. holidays.

Sincerely,

Advanced Medical Practice Management

Steps You Can Take to Help Protect Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. AMPM is located at 25B Hanover Road #250, Florham Park, NJ 07932.

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 bureaus 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is/are approximately [#] Rhode Island residents impacted by this incident.