[PRL Letterhead]

[Name]
Address1
Address2
City, State, Zip]

[Date]

Incident Notice

Dear [Name],

What Happened

On April 12, 2022, Practice Resources, LLC ("PRL"), which provides billing and other professional services to a number of healthcare entities, was subject to a ransomware attack (the "Incident"). With assistance from third-party experts, PRL took immediate steps to secure its systems and investigate the nature and scope of the Incident. As part of its extensive investigation, PRL worked diligently to identify any protected health information ("PHI") and personally identifiable information ("PII") that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about June 5, 2022, PRL determined that the Incident may have impacted PHI or PII related to you. We have not found any evidence that your information was misused.

What Information Was Involved

The Incident may have resulted in unauthorized access to or acquisition of your name, home address, dates of treatment, health plan number, and/or medical record number.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we have arranged for IDX to provide you [12 months/24 months] of free credit monitoring and related services. To enroll, please visit https://app.idx.us/account-creation/protect or call [TNF]. Your enrollment code is [XXX]. To receive these services, please be sure to enroll by [enrollment deadline].

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, we have implemented a series of cybersecurity enhancements and will soon roll out others.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

We are providing this notice on behalf of entities to which we provide professional services. Those entities are listed here: https://www.prldocs.com/wp-content/uploads/2022/07/List-of-Entities-on-Whose-Behalf-Practice-Resources-LLC-Is-Providing-Notice-of-Data-Incident-UPDATED.pdf. If you have questions or concerns, please call our dedicated assistance line at [Phone Number], [Days and Times of Service]. We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

David Barletta
President / Chief Executive Officer
Practice Resources, LLC

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

   - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
   - You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022
(866) 349-5191	(888) 397-3742	(800) 680-7289
psol@equifax.com	Databreachinfo@experian.com	https://tudatabreach.tnwreports.com/
www.equifax.com	www.experian.com/	www.transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement or the attorney general, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

4. *Rhode Island Residents:* You may contact and obtain information from and/or report identity theft to your state attorney general at:

   Rhode Island Attorney General's Office
   150 South Main Street
   Providence, RI 02903
   Phone: (401) 274-4400
   Website: www.riag.ri.gov

   You have the right to obtain a copy of the applicable police report, if any, relating to this incident. You may want to place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, please follow these instructions:

   - Equifax: https://help.equifax.com/s/article/ka137000000DSDjAAO/How-do-I-place-a-security-freeze-on-my-Equifax-credit-file
   - Experian: http://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/
   - Transunion: https://www.transunion.com/credit-freeze/place-credit-freeze

Mailing addresses for the credit reporting agencies are provided above. Credit reporting agencies charge a $5.30 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include: (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, Social Security number, and date of birth; (iii) if you have moved in the past five years, the address of each residence you lived at during that time period; (iv) proof of current address, such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable, (vi) payment by check, money order, or credit card (Visa, Master Card, American Express, or Discover cards only.)

You can also place a fraud alert with the credit reporting agencies. This will flag your file with a statement that says you may be a victim of fraud and that creditors should phone you before extending credit. To place a fraud alert on your credit file call the fraud department of one of the three credit reporting agencies – Experian, Equifax, or TransUnion (see above). When you request a fraud alert from one agency, it will notify the other two for you. You can place an initial fraud alert for 90 days, and may cancel the fraud alerts at any time.