[[COMPANY]
LETTERHEAD]

[Insert name]
[Insert address]

Dear [**Insert name**],

On August 22, 2016, Francisco Jaume, D.O. (the "Practice"), discovered it was the target of a ransomware attack which affected its server. Our server contains certain data elements of personal information for the Practice's patients, including you, such as names, addresses, medical information, and Social Security numbers. While we are currently unaware of any unauthorized use or access of the information maintained on the server, pursuant to The Department of Health and Human Services Office of Civil Rights' ("HHS OCR") guidance, we are providing notice to all individuals potentially affected by the ransomware. We apologize for any inconvenience this may cause you.

Immediately upon learning of the incident, we commenced an investigation to determine the scope of this incident and identify those affected. Additionally, we were required to engage a third party expert to assist in decrypting our server and ensuring the server was no longer subject to the ransomware. As mentioned, we are not aware of any improper use of the personal information which was contained on our server. Nonetheless, we are sending this advisory to you and other individuals to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution we have arranged for Equifax Personal Solutions to help protect your identity and your credit information by providing you with 12 months of Equifax Credit Watch Silver identity theft protection at no cost to you. **To receive these services you must enroll with Equifax Credit Watch within 60 days of the date of this letter.** You may contact Equifax Credit Watch immediately for purposes of (i) enrolling in the program, (ii) assisting you in learning more about identity theft solutions, and (iii) answering some of your questions regarding the incident.

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- Wireless alerts and customizable alerts available.
- One copy of your Equifax Credit Report.™
- $25,000 in identity theft insurance with $0 deductible, at no additional cost to you. †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalize identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality *

How to Enroll

To sign up online for online delivery go to www.myservices.equifax.com/silver

1. Welcome Page: Enter the Activation Code provided at the top of your letter in the "Activation Code" box and click the "Submit" button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

We treat all sensitive employee information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring.

If you have questions or concerns regarding this incident you should call **[Insert number],** Monday through Friday 9 am EST to 9 pm EST. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

Jennifer Schultz, Office Manager

What You Should Do to Protect Your Personal Information

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

1. Contacting 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.
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.transunion.com

2. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. 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. 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 police and you also can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

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

4. If you believe you are a victim of identity theft you should immediately report same to law enforcement.

5. *For Maryland Residents*: For more information on identity theft please contact Maryland's Office of the Attorney General at: Honorable Brian E. Frosh, Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.oag.state.md.us, or by calling (888) 743-0023.

6. For *North Carolina Residents*: For more information on identity theft please contact either the Federal Trade Commission at the contact information provided above, or North Carolina's Attorney General's Office, Address: 9001 Mail Service Center, Raleigh, NC 27699-9001; Telephone: (919) 716-6400; Fax: (919) 716-6750; website: www.ncdoj.com/