Dear Attorney General Office,

I am emailing to report a data encryption event that we experienced at our medical practice. Per the information highlighted below from your site, we are understanding this to be the proper method to report the incident. We have filed a report to the Department of Health and Human Service's Office for Civil Rights, and are also notifying media of the event and the attached notice to our patients. The attached notice give the details of the event and the steps we have walked through.

If you have further questions and or need additional information please let us know.

Sincerely:

Columbia Surgical Specialists, P.S.

COLUMBIA SURGICAL SPECIALISTS

Notice of Data Encryption Event

March 7, 2019

Addressee
Address
City/State/Zip Code

Dear **:

What Happened

On January 9, 2019, Columbia Surgical Specialists, P.S. became aware of the unauthorized access to its electronic systems in the form of a ransomware attack. While the Company believes that no data was acquired, disclosed or used by the unauthorized persons, certain information about you could have been exposed and we believe it is important that you be made aware of this incident.

We know this type of event is unnerving, and we sincerely apologize for any distress this may cause you. The health, safety and security of you, our patients, is our paramount concern. That includes the safety and security of your personal information.

What Information Was Involved

The encrypted files/systems contained information about medical services and patients which the Company is legally required to track. The files may have contained your name and, potentially, drivers' license, social security number and other protected health information.

After a thorough examination of our systems, Intrinium, our IT security provider, concluded:

> *At this time, Intrinium does not believe there to have been data egress, but due to the nature of the ransomware and how the infection first began, there cannot be a guarantee.*

Put another way, the data security experts went through our systems with a fine-tooth comb, and they believe your information was not obtained by the intruder, but they can't guarantee that. Thus, while we believe the risk to you is very low, we are notifying you out of an abundance of caution.

What We Are Doing

We want to assure you that we took immediate action to evaluate the extent and nature of the intrusion and to address the source as soon as the vulnerability was discovered, and we are continuing to review our internal protocols and procedures to prevent this from happening again.

As required by federal law, we have also reported this occurrence to the Department of Health and Human Service's Office for Civil Rights and, because of the possible extent of the incident; we have reported it to the local news media and the Washington State Office of the Attorney General, as required by applicable State law.

Why Did We Wait Until Now to Notify You?

We've often asked that very question when we see news reports about data crimes. We've learned this type of attack unfolds slowly, in fits and starts, and thus the IT experts investigating the situation find bits of evidence that they piece together to learn what happened, and determine the current status. When those pieces became clearer, we reported Intrinium's findings to the authorities, as required. We have worked diligently to make the proper notifications as soon as possible without causing undue alarm with inaccurate information. Along with the forensics experts at Intrinium, we are working with federal and state officials, our attorneys and law enforcement.

Your IT Security Firm Called It "Ransomware." Does That Mean You Paid Money?

Yes, we paid $14,649.09. We received notice from the people that encrypted the files just a few hours before several patients were scheduled for surgeries, and they made it clear we would not have access to patient information until we paid a fee. We quickly determined that the health and well-being of our patients was the number one concern, and when we made the payment they gave us the decryption key so we could immediately proceed unlocking the data. (Again, we believe the information was locked, but not obtained, by the perpetrators). The payment came from the doctors who own Columbia, and will not be passed on to our patients.

Who is affected?

In compliance with government reporting requirements, we initially informed the Department of Health and Human Service's Office for Civil Rights that information of up to 400,000 patients were encrypted – however, after further investigation, the actual number of potentially affected patients is substantially smaller. Although our outside forensic review did not identify any data breach, out of concern for our patients, we are informing all patients of a potential breach.

What You Can Do

At this time there is no evidence that your information has been misused and the Company believes that no data was acquired, disclosed or used by any third party. Instead, as is the nature of ransomware, it is the Company's belief based on available information that certain files were simply corrupted with unauthorized encryption measures to prevent the Company's temporary use or access of that data. If you have any questions you may call (866) 219-2642. Our representatives available at the toll-free number have been fully versed on the incident and can answer questions or concerns you may have regarding this letter.

On behalf of everyone at Columbia, we want to apologize to you. We value a strong relationship with our patients. We know the foundation of that relationship is built on trust, and that we need to roll up our sleeves and work daily to regain that trust. You have our word that we will.

Sincerely,

Columbia Surgical Specialists, P.S.