Nevada Orthopedic & Spine Center, LLP ("NOSC") is providing this notice as part of its commitment to patient privacy. NOSC takes patient privacy very seriously and it is important to us that patients are made fully aware of any potential privacy issues.

**I. BACKGROUND**

NOSC uses outside vendors to provide its services to patients as permitted by our policies and applicable law. One of these vendors, NetGain Technology, Inc. ("NetGain"), is a third-party cloud storage provider that hosts NOSC's electronic health record applications. NetGain represents itself, as a trusted and reputable cloud storage company, having significant experience in the healthcare space and familiarity with the security requirements for maintaining confidential healthcare records.

On December 3, 2020, NetGain provided its clients with notification of a security incident. According to NetGain, after completion of a thorough investigation with law enforcement and a cybersecurity firm, Charles River Associates, it determined that NetGain was the victim of a ransomware attack.[1] On January 15, 2021, NetGain informed NOSC of their being involved in the attack. It was not until January 19, 2021, that NOSC was able to confirm the data included in the breach.

NetGain states it first discovered the breach on November 24, 2020, with the earliest possible date of incursion being September 23, 2020. NetGain chose to pay the demanded ransom, to the person(s) responsible for the attack, without NOSC's knowledge or approval. NetGain has assured NOSC that all data has been recovered with those responsible for the attack having certified its destruction and no retained copies. NetGain has not yet provided any information to verify these statements.

**II. POTENTIALLY AFFECTED DATA**

Upon review of the recovered data, it was determined that the compromised data may have contained full or partial: first and last names, dates of birth, billing information, social security numbers, telephone numbers, mailing and billing addresses, e-mail addresses, patient and record identifiers, information relating to treatment (including billing and diagnosis codes, and the dates and locations of treatment), information contained within state-issued photo identifications (including, in addition to the information identified above, biometric information such as height, weight, organ donor status, and appearance), and insurance cards containing patient names and/or beneficiary numbers.

**III. WHAT NOSC IS DOING TO RESPOND**

NOSC is keenly aware of how important personal information is to its patients. NOSC is committed to providing quality care, including protecting patient information. NOSC wishes to assure its patients that it has policies and procedures in place to protect patient privacy (and requires its vendors to do the same). NOSC regularly reviews and enhances these policies and procedures with a view toward its patients' best interests. NOSC has notified the United States Department of Health and Human Services, and its Office for Civil Rights, in order to keep relevant authorities informed regarding this incident. NOSC will continue to examine their relationship with NetGain.

In addition, NetGain has represented to NOSC that it has taken at least the ten (10) following steps to prevent future incidents: (1) blocked identified malicious IP addresses, (2) enabled international Geo-fencing for Azure-hosted environments,(3) performed additional hardening of network security protocols surrounding their support environment, (4) reviewed and restricted access rights for all privileged accounts, (5) deployed additional log monitoring across all servers, (6) audited and strengthened their access management policies, (7) performed additional hardening of network security rules and protocols to restrict lateral movement across environments, (8) reset passwords, (9) deployed new endpoint protection software (SentinelOne) across all servers, (10) and implemented Managed Detection and Response services (with SentinelOne) for proactive threat monitoring and notifications. Anyone seeking **additional information** regarding NetGain is encouraged to visit **netgaincloud.com**.

**IV. STEPS AFFECTED INDIVIDUALS MAY TAKE**

NOSC encourages affected individuals to be vigilant in monitoring their account statements, credit reports, and explanation of benefit forms. Patients may wish to place a fraud alert on their credit report so that it will be easier to challenge and remove improper entries. Patients observing suspicious activity on their credit report are advised to contact the responsible institution or credit reporting bureau to dispute the activity and take other appropriate action. A free annual credit report can be obtained from

[1] For more information about ransomware, please read this Fact Sheet from the Department of Health and Human Services. Available at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (*last accessed* Feb. 10, 2021).

each of the three major credit reporting bureaus by visiting www.annualcreditreport.com, calling 877-322-8228, or contacting the major credit reporting bureaus at:

**Equifax**
P.O. Box 105069
Atlanta, GA 30348
800-685-1111
www.equifax.com

**Experian**
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

**TransUnion**
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

In addition to the three major credit reporting bureaus, the **Federal Trade Commission** ("FTC") can assist with information regarding identify theft, fraud alerts, security freezes, and steps to protect information. The FTC's address is 600 Pennsylvania Ave NW, Washington, DC 20580, their toll-free number is 877-438-4338, and the FTC's relevant website is www.identitytheft.gov.

Patients, and their legal representatives or guardians, may contact us with any questions and/or concerns by email at HIPAA@nevadaorthopedic.com or by phone at our toll-free number (833) 638-1693.