**A Notice to Patients**

San Gorgonio Memorial Hospital ("SGMH") is committed to protecting the security and privacy of our patients' information. This notice concerns a cybersecurity event that may have involved some of that information

On November 10, 2022, we identified unusual activity within our computer network. We immediately initiated our incident response protocols, which included isolating and shutting off select systems. We also began an investigation with the assistance of a third-party forensic firm. The investigation determined that an unauthorized party accessed our network between October 29, 2022 and November 10, 2022 and, during that time, accessed some of the documents on our system. On November 14, 2022, we discovered that some of those documents contained patient information.

Our investigation into the documents involved in this incident is ongoing. However, at this time, we have identified documents containing patient names, addresses, dates of birth, medical record numbers, visit ID numbers, and/or clinical information, such as dates of service, provider names, and/or department names. In some instances, patients' Social Security numbers, drivers' license numbers, financial account information, and/or health insurance information may have also been reflected in the documents involved.

On December 7, 2022, we mailed notification letters to individuals whose information was contained in the documents initially identified as impacted. Upon completion of our ongoing review, we will mail notification letters to additional individuals whose information is contained in affected documents and for whom we have sufficient contact information. We have also established a dedicated, toll-free call center to answer patients' questions. If you have questions about the incident, please call (855) 504-4431, available Monday through Friday, from 6:00:00 a.m. to 3:30 p.m. Pacific Time. For those whose Social Security numbers and/or drivers' license numbers are identified in the affected documents, we are offering complimentary credit monitoring and identity protection services. We also note that it is always a good idea to review the statements you receive from healthcare providers and health insurers. If patients see services that they did not receive, they should contact the provider or insurer immediately.

To help prevent something like this from happening again, we have implemented additional safeguards and technical security measures to further protect and monitor our IT system.

We sincerely regret any concern or inconvenience this incident may cause. We are committed to the privacy and security of patient information and look forward to continuing to serve our community.