UMC Responds to Privacy Incident Involving Third-Party Health Information Exchange

University Medical Center of Southern Nevada (UMC) is notifying approximately 1,200 patients affected by a privacy incident involving specific external health care entities that may have inappropriately accessed information through a nationally recognized, secure health information exchange framework. The incident was not related to UMC's internal systems.

It is important to note that UMC is not aware of any misuse of patient information related to this incident. In support of its commitment to safeguarding the information of patients, UMC is offering complimentary identity theft protection services to the relatively small group of patients affected by this incident. UMC cares for hundreds of thousands of patients each year across its hospital campus and clinic locations in Southern Nevada.

On January 13, 2026, UMC's electronic health record vendor, Epic Systems Corporation (Epic), notified UMC of concerns involving certain external health care organizations that accessed patient information through Epic's Care Everywhere and Carequality platforms. These platforms are widely used, nationally recognized, secure systems that allow health care providers to exchange medical records electronically for treatment and other permitted purposes under the Health Insurance Portability and Accountability Act (HIPAA). They also support the federal interoperability requirements established under the 21st Century Cures Act, which promote the secure, seamless and lawful exchange of electronic health information across health systems.

Epic informed UMC that a third-party Epic Carequality implementer that managed the access to these networks allegedly enabled certain health care entities to request and obtain patient records through the Carequality framework. Epic has initiated litigation in federal court against some of these entities as a result of this matter. Based upon Epic's review and subsequent legal filings by Epic, there are allegations that some of these entities may have accessed patient records without a valid treatment, payment or health care operations purpose. The allegations remain subject to ongoing legal proceedings.

UMC did not authorize or direct any of the alleged improper access to patient records. The access occurred through a lawful, federally supported medical record exchange framework designed to support patient care. There is no indication that UMC's systems were compromised, breached or that any cybersecurity safeguards failed.

After receiving notice from Epic, UMC worked with Epic to conduct a review to determine whether any UMC patients were affected. UMC's review identified approximately 1,200 patients whose information was accessed through the identified platforms. The information accessed may have included: patient names; medical record numbers; dates of service; and clinical information related to visits, diagnoses, medications and/or treatment.

Social Security numbers, financial account numbers, credit card numbers, and other financial information were **NOT** involved.

Upon receiving notification from Epic, UMC reviewed Epic's investigation findings and technical reports, conducted an internal review of disclosures related to the affected platforms, and confirmed that UMC's internal systems were not compromised. In addition, UMC confirmed that the connections for the suspected entities to the Carequality platform were suspended to prevent further access.

UMC is offering complimentary identity theft protection services through IDX to all patients affected by this incident. These services include 12 to 24 months of credit and CyberScan monitoring, a $1 million insurance reimbursement policy and fully managed identity theft recovery services. Affected patients will receive letters with detailed information about how to enroll in these complimentary services.