Notification of Data Security Incident

University of Mississippi Medical Center Notifies Individuals of Data Security Incident

University of Mississippi Medical Center ("UMMC") is committed to maintaining the privacy and security of personal information. UMMC recently notified individuals of a data security incident involving unauthorized access to UMMC's network environment.

UMMC discovered a data security incident on or about February 19, 2026. Upon learning of this issue, UMMC immediately commenced a prompt and thorough investigation. As part of the investigation, UMMC engaged external cybersecurity professionals who regularly analyze these types of situations to help determine the extent of any compromise of the information on UMMC network. Following its investigation, UMMC discovered on October 20, 2026, that the impacted systems, which may have been accessed and/or acquired between February 11, 2026, and February 19, 2026, contained personal and/or protected health information. The data involved includes full names in combination with dates of birth, driver's license numbers, Social Security numbers, health insurance information, prescription information, medical record numbers, diagnosis/conditions, lab results, employment related information, medications, credit or debit card numbers, financial account numbers, username and password, passport numbers, military or other US Federal ID number, mother's maiden names and other medical information. Not all data elements were impacted for every individual.

UMMC has no evidence that any data has been misused. However, out of an abundance of caution, on November 2, 2026, UMMC is sending notification letters in accordance with state and federal law to each potentially affected individual for whom they have a last known address. UMMC is providing notified individuals with best practices to protect their information and offering complimentary credit monitoring services for those who had their Social Security number impacted. UMMC encourages impacted individuals to take actions to help protect their personal information. These actions include placing a fraud alert and/or security freeze on their credit files, and/or obtaining a free credit report. Additionally, individuals should always remain vigilant in reviewing their financial account statements, explanation of benefits statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities.

UMMC remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it, including continually evaluating and modifying its practices and internal controls.