MEDICAL COLLEGE OF WISCONSIN

Notice of Security Incident

The Medical College of Wisconsin (MCW) has notified certain patients about a recently discovered security incident involving a limited number of MCW employee email accounts.

MCW learned that a small number of faculty and staff were victims of a spear phishing attack to their email system. Phishing is defined as the activity of defrauding an online account holder of institutional, financial or personal information by posing as a legitimate company, organization or individual through the use of email. Spear phishing is an email targeting a specific individual, organization, or business sent to a very small number of individuals to avoid detection.

Upon discovering the issue, MCW promptly disabled the impacted email accounts, required password changes to the compromised accounts, maintained heightened monitoring of the accounts and commenced an investigation. As part of its investigation, MCW retained an independent computer forensic firm to analyze the extent of any compromise to the email accounts and the security of the emails and attachments contained within them.

Since completing the investigation and manual document review, on September 20, 2017, MCW concluded that an unauthorized third party accessed a limited number of email accounts belonging to MCW employees that contained patients' protected health information. The investigation further determined that the compromise of the email accounts occurred between July 21, 2017 and July 28, 2017, but the forensic firm could not definitively conclude if any information was actually accessed, viewed, downloaded or otherwise acquired by the unauthorized user.

The compromised email accounts at issue contained either one or more of the following: patients' names, home addresses, dates of birth, medical record numbers, health insurance information, date(s) of service, surgical information, diagnosis/condition, and/or treatment information. Social Security numbers and bank account information for a very small number of patients were also contained within the affected email accounts.

To date, MCW is not aware of any reports of identity fraud, theft, or improper use of the information as a result of this incident, but provided notice out of an abundance of caution. Notified patients have been provided with best practices to protect their information. It also is recommended that affected patients review the statements that they receive from their health insurance providers and follow up on any items not recognized. Credit monitoring and identity theft restoration services have been provided to those individuals whose Social Security numbers were potentially compromised.

MCW is committed to maintaining the privacy of patient information and continually evaluating and modifying its practices and procedures to enhance appropriate security and privacy measures to prevent recurrence of this incident, including conducting ongoing cyber awareness training for its workforce and regularly updating its system security and firewalls.

We were unable to locate certain potentially affected individuals, and are providing this notice on our website to notify those individuals of this incident. If you did not receive a notification letter in the mail from MCW and you are concerned that your personal information may have been contained within the compromised email accounts, please call MCW's dedicated, toll-free call center at 1-844-666-7416, Monday through Friday between 8:00 am and 8:00 pm Central Time. The call center will confirm whether or not your personal information was included in this incident.

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Protecting Your Health Information.

We have no information to date indicating that your Protected Health Information (PHI) involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.