MEDICAL COLLEGE OF WISCONSIN

[redacted]

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>:

I am writing to provide you with important information about a recent incident involving the security of some of your personal information that you supplied to us at affiliated hospitals or clinics as a result of the services we provided to you. We wanted to provide you with information regarding the incident and let you know that we continue to take significant measures to protect your information. The privacy of your personal information is of utmost importance to the Medical College of Wisconsin ("MCW").

As a large organization, MCW is often the target of hackers and scammers looking to steal information through "phishing" and "spear phishing." 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.

We recently learned that a limited number of our employees at MCW were victims of a spear phishing attack to our email system. Upon learning of the issue, we promptly disabled the impacted email accounts, changed the passwords to those accounts and maintained heightened monitoring of the accounts to ensure that no other suspicious activity was taking place. In addition, we simultaneously commenced an investigation of the incident and 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 our investigation and manual document review, on September 20, 2017, we concluded that an unauthorized third party accessed a limited number of email accounts belonging to MCW employees. The forensic 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 what information within the accounts, if any, was ***actually*** accessed, viewed, downloaded or otherwise acquired by the unauthorized user.

Further, based on the investigation conclusions, we have devoted considerable time and effort to determine what information was contained in the affected email accounts. We conducted a sophisticated review of each email and attachment contained within the impacted email accounts that was forensically identified as having contained personal or protected health information to ensure accuracy and confirm those potentially impacted. Based on our review, we can confirm that the compromised email accounts contained either one or more of the following: your name, date of birth, home address, medical record number, health insurance information, date(s) of service, surgical information, diagnosis/condition, and/or treatment information. Your Social Security number was **not** contained within the compromised email accounts.

To date, we are not aware of any reports of identity fraud, theft or improper use of your information as a direct result of this incident. Due to the complexity of the intrusion, however, we cannot conclusively determine whether the unauthorized user actually acquired or viewed any of your information. Out of an abundance of caution, we wanted to make you aware of the incident. To the extent it is helpful, we have provided steps you can take to protect your health information on the following page.

On behalf of MCW, please accept our apology that this incident occurred. We are committed to maintaining the privacy of our patients' information and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of our patients' information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against potential misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.

Sincerely,

[redacted]

[redacted]

Medical College of Wisconsin

– 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.