MEDICAL COLLEGE OF WISCONSIN
AFFILIATED HOSPITALS

To: All Housestaff

From: Kenneth B Simons, MD
Executive Director and DIO

Re: Outlook Application

Dear Housestaff:

The protection of patient privacy is one of the most important responsibilities a physician has. The use of electronic devices has become a routine part of both our personal and work lives, and while they are incredible tools, mobile devices can easily lead to breaches of patient information. Housestaff need to understand that there are serious consequences if protected health information is breached through the loss or theft of an electronic device that has not been encrypted or through any other means.

All MCWAH housestaff are required to complete HIPAA Privacy and Security Training, as well as sign an attestation indicating that they understand the importance of maintaining the privacy and security of all protected health information. Housestaff are further required to protect all devices used to access or store MCW, affiliated hospital or patient electronic protected health information by installing the MCW approved encryption application (currently the Outlook app) whether the device is personally owned or provided by an MCW Department or MCWAH Program. Housestaff often wonder if private information from their phone can be tracked. No one within MCW is permitted to view or track:

- Personal email (e.g. Hotmail or Gmail)
- Text messages
- Phone call or internet browsing history
- Your location (unless you or your carrier enable location tracking)
- Applications not delivered or managed by MCW that are installed on a personally owned device
- Information within any app on the device (Facebook, Twitter, Evernote, Instagram, Dropbox, etc.), regardless of who owns the device

In order to access the websites below, your Program Coordinator will need to set up Domain access for you. This will be done by July 1st. If you have any questions, please contact your Program Coordinator.

Installing the Outlook App

- Navigate to your device's store *(**App Store** for iOS, **Play Store** for Android).*
- Search for **Outlook.**
- Select the **Microsoft Outlook** app *(NOT the **OWA** app, as this is not compatible with MCW's email environment).*
- Tap **Install.**
- Once installed, open the app.
- Tap **Get Started.**
- Enter your MCW email address. Tap **Continue.**
- Enter your password and desired account description, e.g. "MCW" *(Description is for your reference only)*
- Select the **Advanced Settings** option.
- Enter the following information:
    - Server: **Outlook.office365.com**
    - Domain: **mcw.edu**
    - Username: **<MCW Email Username>**
    - *Note on Android this may be listed as **Domain\Username** on one line*
- Click the **check mark** in the upper right corner.
- You will be prompted to activate Outlook as a device administrator. Click **Activate.**
- You will see a listing of the permissions the app will receive *(Note MCW will not be able to see your personal data).* Click **Activate this device admin app. (**You may also be prompted to install the "Intune Company Portal app before your email will synchronize. This is OK to do.)
- You will now be taken to a tutorial/walkthrough of the Outlook app. You may proceed or skip this step.
- Your MCW email should now appear.

Resources

For questions about the Outlook app and encryption of electronic protected health information, please review the following:

- Encryption for Electronic Protected Information – Mobile Devices (IT.PI.200) Policy
- Electronic Protected Information (EPI) Security Definitions (IT.PI.010)

MCW Information Services is available for questions and assistance. (414) 955-4357 (Option 8).

MEMO FROM ZABLOCKI VAMC PRIVACY OFFICER

Dear Housestaff,

In the fall of 2016 VHA enforced stronger requirements for allowing a physical log book that contains sensitive personal information (SPI) on other individuals. Such a log book may now only exist in physical form if allowed by a regulation put in place by a rule-making agency. ***Since Residents' logs maintained for reviewing and entering ACGME data contain SPI, and there is no regulation backing their continued existence, this information must be maintained in electronic format.***

Each Resident, when granted computer access, is given an apportionment of personal network drive space that is secure and accessible from practically any VA computer (including through Virtual Private Network access). This space, on the user's "U: drive," has restricted access. A password-protected Excel sheet can be used to track SPI required to ensure accurate information is input to ACGME's portal and to verify that patient medical record information is complete. Instructions for creating a password-protected Excel sheet can be found at the following site: https://support.office.com/en-us/article/Protect-an-Excel-file-7359d4ae-7213-4ac2-b058-f75e9311b599. This information must be deleted when it is no longer needed.

As a reminder, VA Sensitive Information (VASI), including identifiable patient health information, must reside within VA's control. Residents must not use personal devices, notebooks, personal emails, or any other non-VA-protected method of transporting or maintaining VASI. Several deviations from this structure in the past have both put our Veterans' information at risk and allowed it to fall into inappropriate hands. In an era where healthcare information is worth 10 times the value of financial data on the black market (up to $50 per record), our tightened responsibilities are more important than ever before.

For any questions about our requirements or for assistance, please contact the facility Privacy Officer, Shanon Cousland, at (414) 384-2000, ext. 41095, or at shanon.cousland@va.gov . For Information Security concerns, you may contact our ISSO's, Kelly Clingaman and Rustine Johnson, at kelly.clingaman@va.gov or rustine.johnson@va.gov .

Shanon Cousland
Milwaukee VAMC FOIA/Privacy Officer
5000 West National Ave
Milwaukee, WI 53295
(414) 384-2000 x41095/42140 (phone)
(414) 389-4193 (fax)

Medical College of Wisconsin Affiliated Hospitals, Inc.

Dear Housestaff,

Please read, sign and return this document to the Medical College of Wisconsin Affiliated Hospitals, Inc. (MCWAH) Office.

As a physician you have an ethical duty to keep patient information confidential. Additionally, Wisconsin law and the Federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), along with its Privacy Regulation, prohibit healthcare providers from disclosing patients' protected healthcare information, except upon written authorization by the patient or as otherwise permitted by law.

Under the HIPAA Security Regulation, hospitals and other healthcare providers are required to have the capacity to determine who is accessing their patients' protected healthcare information; you should know that hospitals electronically monitor access. Failure to maintain patient confidentiality, accessing patient information without a need to do so for your work, failure to properly secure protected health information or any other violation of a Medical College of Wisconsin (MCW), MCWAH or participating site's privacy or security policy, may result in disciplinary action against you. In addition, if a violation occurs, hospitals may terminate your system access or take other appropriate action.

Some general guidelines:

- Access patient information only if you need that information to do your work.
- Share or discuss patient information only if it is necessary to do your work.
- Never share your identification number or password with anyone.
- Follow the hospital's or healthcare provider's policies on confidentiality and privacy.
- Log off your computer session when you are not by your workstation.
- Ensure confidentiality when you handle protected healthcare information.
- If you need clinical information for educational purposes, only use information that has been de-identified in compliance with the hospital's or clinic's policies.
- When using electronic devices or social networking sites refrain from using descriptions of patients or patient related scenarios. Descriptions may violate Federal law and regulations.
- Never take photos or images of patients without prior written authorization from the patient or his/her legal representative.
- Never take paper containing protected healthcare information out of a hospital or training facility

Confidentiality of Proprietary and Research Information

I may have access to proprietary and research information belonging to either MCW or an affiliate hospital of MCWAH. I understand that such information is strictly confidential.

I have received and read the MCW booklet titled Privacy of Health Information. I understand there are rules regarding the use and disclosure of patient protected healthcare information and I agree to abide by such rules and keep protected healthcare information confidential.

All mobile devices used to access or store MCW, affiliated hospital or patient electronic protected information must be encrypted using the MCW approved application whether the device is personally owned, provided by a MCW Department or a MCWAH Program. Please see MCW policy Encryption for Electronic Protected Health Information-Mobile Devices for further information.

I understand and agree that it is my personal responsibility and obligation to protect all mobile, electronic devices such as tablets, smartphones, and laptops that I use for work or patient care using the MCW approved application.

I further understand that a failure to keep protected healthcare information confidential or a breach of privacy associated with a lost or stolen electronic device that was not protected, as required by MCW and MCWAH policy, may result in termination from my training program.

Additionally, I agree to keep all proprietary and research information confidential.

_____

Print Name

_____ _____

Signature **Date**