Information Security Awareness Message
4/30/2010

SCHOOL OF DENTISTRY
UNIVERSITY of WASHINGTON

School of Dentistry Staff, Students and Faculty:

Practicing Security Awareness and following our HIPAA policies is the best way we can protect our patients' confidential information. Our patients have put their trust in us and we are committed to taking the greatest care with their private information. Security Awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical and, especially, information assets of that organization. Please take the time to read the following reminders and make sure they are part of your daily UW routine.

Email Practices

- **No PHI (protected health info) in subject lines**
- **Only include minimum PHI necessary in message**
- **Double check addresses before sending confidential messages**
- **Scan all clinically relevant email into axiUm**
- **The following email signature/footer is required when communicating PHI:**

  The above email may contain patient identifiable or confidential information. Because email is not secure, please be aware of associated risk of email transmission. If you are communicating with a UW School of Dentistry Provider or Researcher via email, your acceptance of the risk and agreement to the conditions for email communications is implied. See the Agreement for Electronic Correspondence at https://dental.washington.edu/compliance/hipaa/agreement-for-electronic-correspondence/.

  Confidentiality Notice: This e-mail message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, distribution or copying is prohibited. If you are not the intended recipient(s), please contact the sender by replying to the e-mail and destroy/delete all copies of this e-mail message. See our Notice of Privacy Practices at https://www.dental.washington.edu/compliance/hipaa.

- **Using external email systems exposes confidential data**

  Auto-forwarding to or emailing with non-UW accounts puts confidential information at risk. School of Dentistry Security Policy SEC-03.02 (adopted from UW Medicine) prohibits School workforce (faculty, staff, volunteers and students) from setting UW email to automatically forward to non-UW or personal email accounts.

  The following UW and affiliate email systems all provide the appropriate protections: u.washington.edu, uw.edu, uwpn.org, uwp.washington.edu, cumg.washington.edu, seattlecca.org, fhcrc.org, psbc.org, med.va.gov, and seattlechildrens.org. Engaging in email communications with any email systems not previously listed provides no protection for patient/confidential information.

  If you are currently forwarding your UW managed email, please go to http://myuw.washington.edu/ to change this setting. In the left margin of MYUW homepage, there is an "email" section. By using that section you can "change email forwarding" and remove any auto-forwarding set to non-UW accounts.

- **Using new UW Microsoft Live and Google Apps to forward email violates policy**
  The University of Washington has recently entered into agreements with Microsoft and Google for email, calendaring, and collaboration services for students and alumni. Although these services will be offered to UW faculty and staff, as a School of Dentistry workforce member you MAY NOT forward your UW email to these services or store confidential data on these services.

Copying of data and media disposal

Media is any portable device that is capable of storing electronic data. Examples include USB drives, CD/DVD, external hard drives, tapes, flash memory cards, etc. Once a workforce member removes data from a controlled system it becomes their responsibility to ensure the protection of the data.
PHI (Protected Health Information), PII (Personally Identifiable Information) and passwords stored on media must be encrypted. Media containing restricted or confidential information must be destroyed in such a way to make the data unrecoverable when no longer needed.

Personally owned mobile devices

Mobile devices include laptops, Blackberries, smart phones, or any portable device capable of storing and interpreting data. Mobile devices are of special concern because they are easily lost and attractive to thieves. Personally owned mobile devices must comply with School of Dentistry policies and standards when used for work purposes. The owner of the device is responsible.

- Encryption required when storing PHI, PII or passwords
- No automatic login; require password to logon to the device
- Passwords on these devices must be changed every 120 days
- Patched and up to date operating system

Questions, concerns and potential violations

- Contact our Compliance Director at 543-5331 or compliance@dental.washington.edu.
- Contact your supervisor
- Call the anonymous compliance hotline at 685-5254

By signing this document, I understand and agree to abide by the policies explained above:

Printed Name: _____

Signature: _____

Department/Title: _____

Date: _____

☐ Copy to Workforce Member ☐ Original Filed in Personnel/Student File