**WORKSTATION AND DEVICE USE PROCEDURE**

By the end of this month, every HIPAA workforce member needs to read and agree by signature to follow our BU HIPAA Workstation and Device Use Procedure. This procedure for either [health care providers](http://www.bu.edu/hipaa/forms-for-health-care-providers/) or [health plans](http://www.bu.edu/hipaa/bu-health-plans/) sets out the basic requirements you must follow when using BU or personal workstations – desktops, laptops, mobile phones, tablets – to access, process, or store HIPAA data. Additionally, any personal workstations you want to use for accessing, processing, or storing HIPAA protected health information must have the minimum safeguards required by this procedure and brought to the IT Help Center at Amory Street (West Campus) for verification.

**Which personal workstations must brought to the IT Help Center for verification?** Only workstations you intend to use for accessing, processing, or storing HIPAA protected health information. The clearest example is if the personal workstation will access an electronic medical record (e.g. Valant, eClinicalWorks, Clinicient) or database (e.g., OnBase, Bluelinks, Optum).

**What is HIPAA protected health information (PHI)?** Any information created or received by a BU Covered Component that identifies a patient or health plan enrollee and relates to their health, provision of healthcare, or health plan enrollment. For example, a picture showing a patient’s face without a name is PHI, if it relates to their health or provision of healthcare, and an email or text message to a patient is PHI because their email address or phone number can be used to identify them.

**Do I need to get my mobile phone checked simply because I access Outlook using an app or a web browser on my phone?**

Some workforce members use Outlook to communicate with patients or health plan enrollees, who have requested non-secure email (See [BU HIPAA Policy Section 6.6 Right to Request Confidential and Alternate Modes of Communication](http://www.bu.edu/policies/information-security-home/hipaa_toc/hipaa-individual-rights/)). Workforce members who communicate with patients or health plan enrollees using Outlook need to get their personal mobile phone checked before accessing Outlook on it.

**I only use DataMotion on a BU workstation for communication with patients or health plan enrollees. However, some patients have found my Outlook email address and emailed me. Do I need to get my personal mobile phone checked?** It depends on how you respond. If your practice is to delete the email in Outlook and continue the conversation in DataMotion on a BU desktop or laptop then your personal mobile phone does not need verification, but if your practice is to respond in Outlook then your personal mobile phone does need verification.

**What is the process for getting my personal workstations checked by the IT Help Center?**

First, encrypt and add anti-malware to your personal workstations using our guidance: <http://www.bu.edu/tech/support/information-security/securing-your-devices/>.

The IT Help Center will verify four minimum safeguards:

1. supported and updated operating system,
2. disk encryption,
3. anti-malware set to auto update and scan on desktops and laptops,
	1. Apple mobile phones (not required),
	2. Android mobile phones (Play Protect enabled),
4. auto screen lock to password or code (15 minute max, 2 minute max for phones).

Second, setup an appointment at the IT Help Center by sending an email to ithelp@bu.edu containing the following information:

* Subject: HIPAA Personal Workstation Review
* Body:
	+ Type of workstation(s): mobile phone, laptop
	+ Operating system(s): for example, Windows 10 Pro, iOS11,
	+ Covered Entity: Danielsen/HR-Benefits/SAR PTC/SAR Nutrition/SAR Neuro
	+ Availability for appointment at IT Help Center (179 Amory Street, Brookline)
		- Identify three dates and times during open hours <https://www.bu.edu/tech/contact> (1/2 hour time will be selected)

**Have questions?**

* Contact your [HIPAA Contact](http://www.bu.edu/policies/information-security-home/hipaa_toc/hipaa-appendix-a/), or your HIPAA Security Rule Officer, David Corbett, at corbettd@bu.edu