I'm not really into spring cleaning. Come to think of it, I'm not into summer, fall, or winter cleaning either. But I know I need to put a little effort in from time to time to keep the clutter from building up. Similarly, taking a little time now to clean up my emails and files can prevent a big impact on patient privacy down the road.

What can I do to protect patient privacy?
One of the ways you can help is by getting rid of old emails and paper files, which contain health information (HIPAA or personally identifiable human subject health data) or personal information (Social Security Numbers, checking account numbers, or debit/credit card numbers), you don't need any more and aren't required to be retained pursuant to the BU Retention Policy.

Why should I get rid of files I don't need?
If you have electronic files, they can be subject to a cyberattack – using phishing or other tactics. If you have paper files, they can be improperly accessed by another person (whether intentional or accidental). These events could require us to notify the individual whose information was involved. It could be very time consuming and challenging to try to contact individuals, we may no longer have a relationship with or haven't seen in a very long time. While some data must be kept, we often hold data we don't have to keep - and the worst breach is a breach of data we did not need to keep, and that could have been avoided.

How can I help?
You should move electronic data from your personal devices and email to your HIPAA Covered Component designated repositories. For example, if a patient changes an appointment outside the medical record, the information should be transferred to the medical record, either as a file upload or note, as dictated by your Covered Component procedures. Likewise, electronic research records should be stored on BU storage, not personal locations.

Paper and electronic records, no longer need to be retained per the BU Record Retention Policy should be disposed of as soon as possible. Guidance for the proper way to destroy these records may be found here: https://www.bu.edu/tech/about/policies/1-2-d-1-destruction-of-paper-records-and-non-erasable-media-cd-roms-dvds/ and https://www.bu.edu/tech/services/infrastructure/storage-backup/media-destruction/. BU Information Security also provides two Shred + Recycle Events a year for faculty, staff, and students to bring paper and electronic media to be destroyed.

I am so excited to start. How long do I have to wait?
The BU Record Retention Policy requires medical records to be retained for 20 years, sponsored research for 7, and Human Resources records covered by HIPAA for 7 years after an individual leaves BU. If this doesn't describe your data, see this document: http://www.bu.edu/policies/record-retention-table or consult with your departmental administrators. Keep records for the required retention period, and then delete them as they reach the end of the required retention time frame.

But you don't have to wait to move electronic data from your personal devices and email to your HIPAA Covered Component designated repositories. You can do that now!

If you have questions reach out to: buinfosec@bu.edu or your HIPAA Privacy and Security Officers at hipaa@bu.edu

BOSTON UNIVERSITY

Boston University Information Security
buinfosec@bu.edu
www.bu.edu/infosec