



Dear Colleagues,

No one likes bad publicity so don't let it happen to you! The worst kind of data breach is the kind that did not have to happen. Despite our best intentions, accounts sometimes get compromised. If your email contains personally identifiable information, we may have to notify all of those individuals along with the government. The best protection is not to use email to send patient data. If you have, you should delete it as soon as possible. Note that "identifiable information" doesn't have to be the whole patient record to require reporting. It could be emails with pictures or videos of patients, phone numbers, or even just the dental or medical record numbers.

If you have any emails about patients or human subjects, please move them or the data within the emails to the appropriate repository, then delete them from your email.

What if I need to keep these emails as proof of correspondence with the patient?

Our email system is neither the legal record required by Massachusetts law or an appropriate data repository for human subject data or patient data. If you have questions about how to properly store medical or human subject records, please reach out to hipaa@bu.edu.

Is deleting messages from my Inbox enough?

No, please delete messages in both your “Inbox” and “Sent” folders, then delete them all from your “Deleted Items” folder: <https://support.microsoft.com/en-us/office/delete-email-in-outlook-com-a9b63739-5392-412a-8e9a-d4b02708dee4>.

Why would someone have patient emails in their BU Outlook account?

Clinical units and researchers should communicate with patients and human subjects using DataMotion, Microsoft Teams, or another HIPAA compliant method:

<https://www.bumc.bu.edu/it/infosec/researchcompliance/bu-reviewed-and-cleared-apps/>.

With appropriate waivers, patients and subjects can request to use email instead of these tools, accepting the risks of using this less secure communication method. However, this waiver does not exempt the university of responsibility for notifying the individual and/or the government if we become aware of a breach of our accounts and systems.

If you have any questions or concerns, please contact me or Information Security at buinfosec@bu.edu.

Sincerely,

David Corbett, BUMC Information Security Officer and HIPAA Security Officer



Boston University Information Security

buinfosec@bu.edu

www.bu.edu/infosec