EMAIL BEST PRACTICES
Security Reminder

OCTOBER 2021

Dear Colleagues,

All communication with patients and research subjects poses some risk to the privacy of those individuals. In simple cases, a conversation or message may be overheard, but in other cases our choice of communication method increases the risk that a message will be sent to the wrong recipient: regular email improves our productivity by remembering addresses, but the downside is emails are sometimes accidentally sent to the wrong patient (with a similar email address).

So, what should I do?

Use BU Secure Email service (free to use) and verify patient addresses before hitting send. Email addresses have to be manually entered for each email or manually entered into an address book.

I understand that BU Secure Mail is more secure, but what if a patient requests traditional email or text?

As a provider, you should not be suggesting patients use regular email or text. But if a patient requests to use unsecure email or text, have them confirm understanding, ideally in writing using a standard form.

We have forms for each HIPAA Component and an example form any non-HIPAA clinics or research teams can use to document patient preference here: https://www.bu.edu/hipaa/forms-for-health-care-providers.

What do I need to remember every time I write or respond to an email from a patient or subject?

Verify the email address matches the patient or subject you intend to send the email to. 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