



Dear Colleagues,

A good security program requires everyone to be involved and understand their responsibilities. IS&T, BUMC IT, and Dental IT work hard to ensure our HIPAA servers and devices are secure. But if a HIPAA workforce member leaves a door to a clinic or office area unlocked, shares their password, or discusses patient data inappropriately, an adversary can bypass all the security controls we have implemented.

We urge you to take some time now to review the steps we all need take to keep HIPAA data secure: <http://www.bu.edu/policies/hipaa-indiv-responsibilities-safeguarding-phi/>

Our patients and insureds depend on us to keep their data secure. Please do your part, by understanding and carrying out your responsibilities, and reaching out with any questions to [hipaa@bu.edu](mailto:hipaa@bu.edu).

Sincerely,

David Corbett

BUMC InfoSec Officer and HIPAA Security Officer

BU Information Security



**Boston University** Information Security  
[buinfosec@bu.edu](mailto:buinfosec@bu.edu)  
[www.bu.edu/infosec](http://www.bu.edu/infosec)