Boston University Information Services & Technology
Information Security

Dear Colleagues,

When team members leave, their access needs to be removed immediately to prevent former workforce members from accessing records they should no longer have access to.

Why is removing access so important?

- We have told patients, insureds, and research subjects through Privacy Practice Notices and research consent forms that we will protect their data and only allow authorized individuals to have access.
- Former employee accounts are more susceptible to abuse because former employees are less likely to notice or report suspicious activity.
- Former employees may use information about patients, such as to persuade them to move to a new practice.
- State and federal agencies who enforce HIPAA impose penalties for not immediately removing access: https://www.hhs.gov/about/news/2020/10/30/city-health-department-failed-terminate-former-employees-access-protected-health-information.html.

How is access removed at BU HIPAA Components?

Like most things that are security related - it is a team effort. Generally, HIPAA Contacts/Managers submit an Access Request to provide, modify, or revoke access, that sends an alert to IS&T or Dental IT. IS&T or Dental IT then change the access they control, such as managed computers and network drives. Faculty and staff remain responsible for removing access to applications they control, such as Microsoft apps (e.g., Teams, SharePoint, and OneDrive).

Why is access removal not automatic, without interventions?

University culture often encourages continued access. For example, because we want to maintain relations with former students, alumni, and retirees, their BU Login account is not disabled. So, anyone who has taken a class or retires from BU may continue to have access to BU services after they have left. This makes sense for our academic mission, but not for healthcare and some research activities.

So, please do your part and remember to remove access immediately. We also encourage you to periodically review who has access to ensure any missteps are quickly corrected.

Please reach out with any questions.

Sincerely,
David Corbett
BUMC InfoSec Officer and HIPAA Security Officer

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