Boston University IS&T Information Security

HIPAA Compliant Services

Dear Colleagues,

The HIPAA regulations require that all applications used for any purpose involving insured, research subject, or patient information receive a security risk assessment. At Boston University, this means that BU Information Security has reviewed it and your HIPAA Contact (the person who sent you this message) approves of its use. As an institution we are most efficient if we reuse already approved applications. Go here to see our complete list of reviewed apps: http://www.bumc.bu.edu/it/infosec/researchcompliance/. If there is an application you would like to use that is not listed as HIPAA compliant, please ask your HIPAA Contact to submit a request to bumcinfosec@bu.edu.

Why are some applications considered HIPAA compliant and some are not?

The HIPAA Privacy and Security Rules only apply to covered entities, generally health plans and health care providers who bill insurance companies. Software development companies such as Apple, Google, and Microsoft create apps. Since they are not heath care providers who bill insurance companies, they do not have to comply with HIPAA.

Some companies that create apps, however, are willing to sign a HIPAA Business Associate Agreement, requiring them to comply with the applicable parts of the HIPAA Privacy and Security Rules. Microsoft has signed a HIPAA Business Associate Agreement with Boston University, and many of their services are HIPAA compliant: OneDrive, PowerBI, SharePoint, Stream (video storage), and Teams (HIPAA Zoom alternative that allows cloud recording and chat), among others.

When we have completed a security review and obtained a BAA, we identify the service as HIPAA compliant. Go here to see the complete list of HIPAA compliant services: http://www.bumc.bu.edu/it/infosec/researchcompliance/

What are some common services that are not HIPAA compliant?

Google apps, Apple iCloud, and Grammarly are regularly used by us on personal devices, to store pictures and correct our spelling. What is great in our personal lives is not always great for patient data. For example, many services - including iCloud - prohibit the use of their services to create, receive, maintain, or transmit HIPAA data (https://www.apple.com/leal/internet-services/icloud//en/terms.html).

And while Grammarly may appear to work locally on your personal devices, it is in fact sending everything you type to its own cloud servers for review. This means a copy of any document you use with it is silently sent to Grammarly. Grammarly cannot be used on devices used to access, process, or store HIPAA data because Grammarly will not sign a HIPAA Business Associate Agreement.

Sincerely,
David Corbett
BUMC Information Security Officer and HIPAA Security Officer

BOSTON UNIVERSITY

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