Research Data Security

Storing and sharing Research Protected Health Information (PHI) on Box

Background

Box ™ is cloud-based file storage and collaboration service that has been approved for storing and sharing highly restricted, level 4 data, which includes protected health information (PHI), as defined by the UM information security program. Because of the self-service nature of Box™, certain additional restrictions must be in place to prevent unauthorized access to level 4 data. Those restrictions include limiting folder ownership and setting folder configurations to mitigate accidental data exposure.

Policy

Box folder ownership, when used to store PHI and other forms of highly restricted data, must be assigned to and controlled by a responsible individual (see definitions). Folder restrictions that prevent unauthorized access must also be in place (see procedures below).

Folder ownership establishes clear responsibility for managing access to data and includes tasks such as adding and removing collaborators, allowing or restricting file access, deletion of files when appropriate or necessary, etc.

All responsible individuals who share data via Box must employ the principal of least privilege, meaning that data is not to be shared beyond its intended scope of recipients for the least amount of time required. Data sharing rights must be reviewed on an annual basis, at a minimum. Accounts that are no longer active must be removed from the folder's permissions for access.

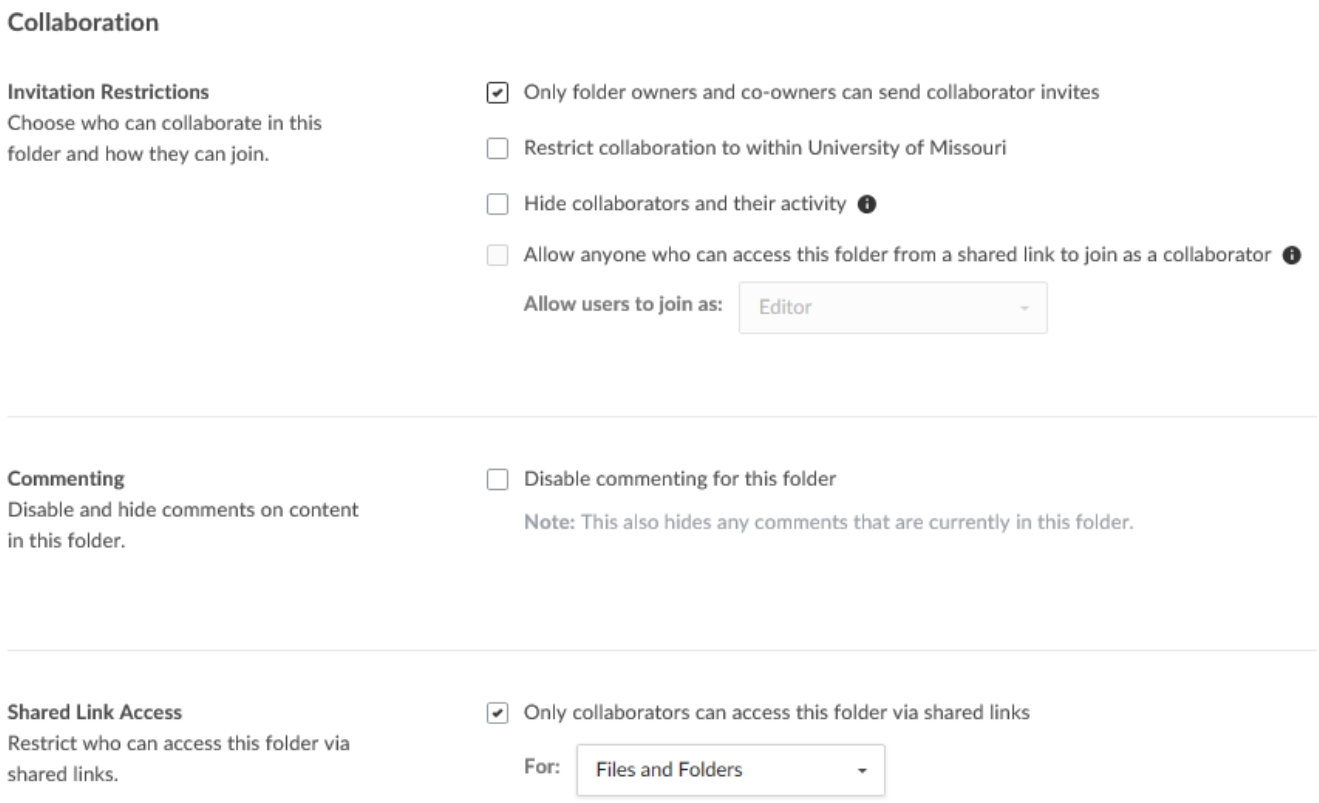
Procedure

When Level 4 data is involved, the folder owner will create a Box folder specific to the topic or project and add the appropriate collaborators.

Establish the following additional folder restrictions:

1) Restrict the ability for non-owners of the folder to add collaborators.
2) Limit access to the folder content via file "links" to existing collaborators only.

See screen shot below:



Folder owners should consider additional restrictions to enhance security, such as "restrict collaborators to within the University of Missouri," when appropriate.

Assistance with Box folder creation and configurations can be obtained through your IT support team.

Definitions

Responsible individual – An individual of sufficiently high level of responsibility, typically a manager, director, principal investigator (PI) or Co-PI or higher level. This individual will typically assign work and be responsible for the final delivery of work product.

Protected Health Information (PHI) – any information, whether oral or recorded in any form or medium that relates to:

- The past, present or future physical or mental condition of an individual; the provision of health care to an individual; or to the past, present or future payment for the provision of health care to an individual; and

- That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual, and shall have the meaning given to such term under Health Insurance Portability and Accountability Act (HIPAA) and the HIPAA regulations, including, but not limited to 45 CFR § 164.501 Privacy of Individually Identifiable Health Information..
- HIPAA/HITECH Protected Health Information (PHI) Identifiers:
  a. Name
  b. All geographic subdivisions smaller than a state (street address, city, county, and precinct) (Note: ZIP code must be removed, but can retain first 3 digits if the geographic unit to which the zip code applies contains more than 20,000 people)
  c. For dates directly related to the individual, all elements of dates, except year (i.e., date of birth, admission date, discharge date, date of death) all ages over 89 or dates indicating such an age
  d. Telephone number
  e. Fax number
  f. Email address
  g. Social Security number
  h. Medical Record number
  i. Health Plan number
  j. Account numbers
  k. Certificate or license numbers
  l. Vehicle identification/serial numbers, including license plate numbers
  m. Device identification/serial numbers
  n. Universal Resource Locators (URLs)
  o. Internet Protocol addresses (IP addresses)
  p. Biometric Identifiers
  q. Full face photographs and comparable images
  r. Any other unique identifying number, characteristic, or code
  s. Genetic Information