Data Sharing for Researchers

Before sharing Confidential Data, confirm:

1) Protocol allows sharing data with this individual, institution, or vendor
2) The recipient institution has signed a Data Use Agreement or vendor has signed a Business Associate Agreement
3) You have selected a secure, approved tool to share the data in compliance with the applicable protocol and agreements (see tools grid below)
4) You have Principal Investigator's permission to use this tool to share data with this individual, institution or vendor

The following grid identifies Partners approved tools for sharing data internally or externally. Researchers must choose a tool that also meets protocol and agreement provisions.

Tool	**Internal**	**External**	**How to Get It**
Syncplicity Enterprise	✓	✓	Purchase a license through the Ergonomics contact for your department
Dropbox Business (Partners) **	✓	✓	Contact the help desk, 6-5085
Partners Secure File Transfer (Accellion)	✓	✓	https://transfer.partners.org
OneDrive for Business (Partners)	✓		Contact the help desk, 6-5085
Shared File Area – shared folders on the Partners network	✓		Contact the help desk, 6-5085

* Syncplicity Enterprise complies with FIPS (Federal Information Processing Standard). NIH and government sponsored studies require use of FIPS compliant tools.

** DropBox for Business at Partners HealthCare is the preferred tool if it complies with your protocol.

- FAQ: (KB0028677)
- Dropbox user guide
- Contact the IS Service Desk for all new Dropbox Business account requests and support.

What if I want to use a tool not on this list for Confidential Data?

- Submit an ISPO Cybersecurity Risk Assessment https://pulse.partners.org/hub/departments/ispo/security_risk
    - Scroll down to the "Request a Vendor Risk Assessment" button, and then click the "request a vendor risk assessment" button.
- Obtain a signed Business Associate Agreement or a Data Use Agreement

Email carries inherent risks that can put your Confidential Data at risk.

1) ***Sending Messages:*** You may use Partners email to send a message. Messages sent externally, however, are not secure UNLESS you type: **"Send Secure"** into the subject line. Typing "Send Secure" into the subject line will protect the information from being intercepted and read or stolen by authorized parties. The recipient of a "Send Secure" email will receive a link to a secure portal where they can read and respond to the message.

2) ***Sharing data sets:*** Do not use email to share data sets (documents, spreadsheets, attachments) classified as Confidential or Institutional Data. See tools above.

When using email, always follow the standards outlined in the "Do" section. Be aware of the email "Don'ts", which compromise data security and may result in reportable research breaches.

Do	Don't
Use "Send Secure" in subject line of email to encrypt messages in transit.*	Send a message with confidential information or institutional information that should remain private without typing "Send Secure" into the subject line.
Use your Partners email to conduct Partners business.	Use non-Partners email to conduct Partners business.
Use collaborators' institutional email addresses.	Send or forward e-mails with confidential or institutional information that should remain private to personal email accounts (e.g., Gmail, Yahoo, Comcast, etc.)
Double check before "Reply All" Always check that you have selected the correct recipients Regularly update group e-mail lists; remove participants who are no longer needed	Let the Outlook use auto-complete option add the wrong name.
Use "Blind Cc" when emailing subjects. Remember you need IRB approval to communicate with subjects via email. You also need subjects' permission to send an email that is unencrypted.	Include multiple subjects on the "To" line.
Include ONLY minimum necessary information.	Attach documents with Confidential Data or Institutional Data that should remain private to emails or meeting invites.

Contacts:
Research Information Security Officer (RISO): Fabio Martins, RISO@Partners.org, 857-282-3704
MGH Information Security Officer (ISO): Toby Tsuchida, ttsuchida@partners.org, 857-282-3518
MGH Privacy Officer: Christine Griffin, cgriffin7@partners.org, 617-643-4028
Questions, comments or to report a Privacy Incident: 617-726-1098.