ONLY ACCESS DATA IF APPROVED & NECESSARY...

- Data access is granted based on your role within the organization and business need for access.
- Only access data specifically required for you to do your job.
- Access only the minimum amount of information that you need for your purpose.
- Assume data requires protection under the law unless it is properly de-identified.

ONLY FOR APPROVED PURPOSES & WITH APPROVED SERVICES...

- Only access data or run reports for projects that have been approved for you to work on.
- Do not share data with any non-Stanford staff or use data for research, publishing, conferences or any other sharing with external parties without approval from the Privacy Office.
- The Stanford data classification for protected health information (PHI) is “High Risk PHI Data.” Only use approved services for handling this type of data.

Taking all needed security steps.

- Never share your access credentials (login IDs and passwords) with anyone.
- Use a strong password.
- Lock or secure your workstation when walking away.
- Use Stanford-approved encrypted devices to access, capture, store, or transmit PHI.
- Use Secure email with sensitive data.

If with Stanford Health Care (SHC), or Stanford Medicine Children’s Hospital (SMCH), take these steps with sensitive data:

- Only store data using the SHC/SMCH secured network.
- Use Stanford Medicine Box or remote access to store and transfer files.
- Engage IT for secure external file transfers.

Review approved services by Stanford data classifications DATACLASS.STANFORD.EDU