

Keeping Your Data Secure

At Penn, using data is an integral part of our research and teaching missions, and data flow is important to many administrative processes as well. But those of us who are not computing experts may need some advice or consulting to help ensure that we keep the data as secure as possible while still being able to use it. If you have concerns about the ways you process or store data, we invite you to contact your LSP or the SAS Information Security team for an individualized SPIA (security and privacy impact assessment) consultation. You may also find these “quick tips” helpful:

- Use caution when considering using a third-party cloud service like DropBox (for example, to collaborate with colleagues outside of Penn). There are serious threats to privacy, and no guarantee of data integrity, with some of these tools.
- Find out whether you have sensitive data lurking on your computer: arrange with your LSP to do an Identity Finder scan.
- Do not assume that email is secure. It isn't. Instead, for sensitive data that you need to share with colleagues, use SAS shared network drives whenever possible. ISC's SecureShare does not provide the same end-to-end security that a shared drive does, but it can be useful for occasional file exchange. A phone call is also more secure than email and can be useful if you only need to communicate a small amount of information.
- Make sure that any paperwork that may contain confidential information (eg payroll data or grade sheets) is physically secure in a locked cabinet in a secure office or other space.

More information is available at yourdata.sas.upenn.edu, or from your LSP.