Questions to ask yourself as you prepare your protocol and communicate your plans to your departmental reviewer and the IRB:

1. **Am I only collecting data that is absolutely essential to my research? Is there any non-essential data being collected?** The most secure data is data that is never collected in the first place. Ask yourself if you really need to collect potentially identifying information to pursue your project. This includes how you collect your data. Do you need to record audio or video? Make sure to explain the necessity of the data collected in your protocol so the IRB understands why all the data points you will request are necessary.

2. **How damaging would my data be to the research subjects if it were released or accessed by others?** Some data isn’t damaging: no one is likely to be harmed if someone else deduces their favorite flavor of ice cream. But if you’re asking questions about more sensitive behaviors, consider what the damage might be to subjects if that data got out. Sensitive data might include information about illegal or sensitive behaviors (drugs, sex, etc.); health records or information about mental or physical illness; or immigration status.

3. **From whom am I trying to keep this information?** Think about who would be in a position to cause negative consequences for your subjects if they gained access to your data. Sometimes that might be an employer, a landlord, the police, a national government, or a subject’s friends and family. You should also think about whether you will be crossing any borders during the process, since that exposes you automatically to additional risk.

**Working with the answers to (2) and (3), consider what level of protection your data needs.**

**If your data necessitates a LOW level of protection, make sure you are still taking best-practices precautions as a digital citizen.**

- Maintain strong passwords on all devices
- Secure phones used for research data with a numerical code rather than a fingerprint or face ID. Use encryption where possible.
- Minimize the number of machines where data is stored: delete data from a phone within 24 hours.
- Upload data to Bryn Mawr’s H: or S: drive or to OneDrive rather than to iCloud or Google Drive (and make sure, if you use your phone to collect data, your phone isn’t automatically duplicating it on iCloud or Google Drive). Backing up to a paid, encrypted service (i.e. Dropbox) could be okay—check with the IRB.
• Do not store research data on public or shared machines.
• Use secure wireless networks (i.e. not airport, Starbucks, or other public connections).
• Turn on full-disk encryption on your personal computer if possible.
• Securely delete data when you are done with the project.
• Do not transport data on hard drives (phone, computer, tablet, external drive, flash drive) across international borders. Your rights are extremely limited at border crossings.

If your data necessitates **HEIGHTENED** precautions, make sure you do the above, plus:

• Store and access research material *only* on devices with full-disk encryption enabled. If you are not using a College-owned computer, what program will you use to encrypt it?
• Researchers working internationally with sensitive data need access to a secure (paid) VPN that they can use to transmit, access, and communicate about their data.
• Make sure you can delete securely. Storing data on Bryn Mawr’s H: or S: drive allows for secure, permanent deletion.

If the data requires **EXTREME** precautions, add these extra measures:

• If possible, edit and access data only through OneDrive, so that unencrypted versions are never downloaded to a researcher’s computer.
• If using OneDrive, talk to the Help Desk to arrange for secure deletion by someone with admin privileges.
• Add a second layer of encryption: individually encrypt research files or folders using a program like BitLocker (PCs) or Keke (Macs).