Best Practices for Maintaining the Security of Research Data

As the researcher, it is your responsibility to safeguard the confidentiality of your research data. A key component of this is consideration of how you collect your data, where that data is stored, and how it is accessed.

General guidance:
The Bowdoin IRB recommends that, whenever possible, data be recorded and stored in a way that minimizes the likelihood that participants could be identified by a breach in security (e.g., hacking, loss or theft of a device that stores identifiable information). For example, you might collect the data in such a way that participants remain anonymous (e.g., by changing the settings in your data collection platform so it does not automatically record name or IP address). When this is not possible, you might separate the identifiers from the data and code the data with a pseudonym or number and then have a separate, confidential file that connects the code to the identifiers.

Collecting and/or storing data electronically:
The College has contracts with for data collection (e.g., surveys), Zoom for videoconferencing (e.g., online interviews and focus groups), and Microsoft O365 for data storage. These agreements ensure adequate data security to store Federal Educational Rights and Privacy Act (FERPA)- and Health Insurance Portability and Accountability Act (HIPAA)-protected information. Bowdoin IT strongly recommends that researchers use these platforms to collect and store their data. When you use these platforms, please sign into them with your Bowdoin credentials and not with a personal account. Personal accounts likely do not have the same level of security as those connected with the College.

At the same time, there may be legitimate reasons why you cannot use these platforms to collect or store your data. For example, you might use a handheld recorder to collect audio or video. In this case, data should be immediately transferred from the recording device to a more secure platform (e.g., Microsoft Office (O365)/One Drive) and deleted from the device on which it was collected. In the case of recordings, we also recommend that you record only what is necessary for the conduct of your study. For example, if you want a transcript of an interview, you should only create an audio recording and not a video recording. If you elect to use alternative online platforms to collect and/or store your research data (e.g., Google Forms, Survey Monkey, Google Drive), your protocol may need additional review. Should this be necessary, you should be prepared for a lengthier review process.

Bowdoin's IT policy recommends that passwords that are at least 12 characters in length and that researchers use multi-factor authentication whenever possible.

Guidance on email communications:
Email is not a secure way to transmit information. Information sent by email can be easily intercepted by third parties. If your study requires that you communicate with participants

via email, participants should be informed that the confidentiality of email communications is not assured.
If you need to share research data with a collaborator, Bowdoin IT recommends that you share it within Microsoft O365. If Microsoft O365 does not serve your needs, please contact Bowdoin IT (itsecurity@bowdoin.edu) to explore other options.

Collecting and/or storing your data on paper:
Physical data should always be stored in a secure location (e.g., a locked filing cabinet).

Who has access to your study data:
It is also important to consider who will have access to your study data. Only individuals who need access to perform their duties on the study should be granted access. If you are unsure how to restrict access to your study data, please contact us at irb@bowdoin.edu. If you intend to share de-identified data with others (e.g., collaborators, in a data repository), this should be clearly outlined in your consent form.

What to do if you have experienced a breach in security:
If you believe your research data has been inappropriately accessed or stolen, you must notify the Bowdoin IRB within 72 hours (irb@bowdoin.edu).

How long to keep your study files:
Your plan for retention of consent forms and other study data should be clearly stated in your protocol and consenting documents (e.g., consent form, assent form, information sheet).

Consent forms
Federal regulations require that signed consent forms be retained and available for inspection for at least 3 years after completion of the research, regardless of the source of funding for your research. It is your responsibility to ensure the safe and secure retention of these records.

Other study data
If your research is externally funded, you should consult with requirements set forth by the sponsor of your research regarding retention of other study data (e.g., federally-funded data must be retained for at least 7 years).

If your research is internally funded or not funded, it is up to you how long you store your other study data.

What to do with study documents if/when you leave the College:

Consent forms
If at the time of your departure, you have consent forms for a project that is active or concluded within the last three years, you are still responsible for maintaining these

documents in a secure and confidential manner until at least 3 years following the conclusion of the research.

If you are a student, please transfer these documents to your faculty advisor prior to your departure.

Other study data
If your research is externally funded, you should comply with the requirements set forth by your sponsor and the plan outlined in your grant application (e.g., a copy of all federally-funded research data must be retained by the College).

If your research is internally funded or not funded, you may destroy the data or take it with you when you depart, consistent with the plan described in your IRB protocol and/or closure form. Please note that if the data you take with you is identifiable, then any future analyses done with that data would require an active IRB approval. You could pursue this approval at your new host institution and/or at an IRB that allows outside investigators to use their services. If, however, the data you take with you is not identifiable, then future analyses would not be considered human subjects research and would not need IRB approval.

If you are a student, please ask your faculty advisor how you should retain or dispose of your data.

Questions?
For more information, please see guidance on Bowdoin IT policies and standards. For general questions contact irb@bowdoin.edu. For information technology questions, please contact Bowdoin's Chief Information Security Officer (itsecurity@bowdoin.edu).