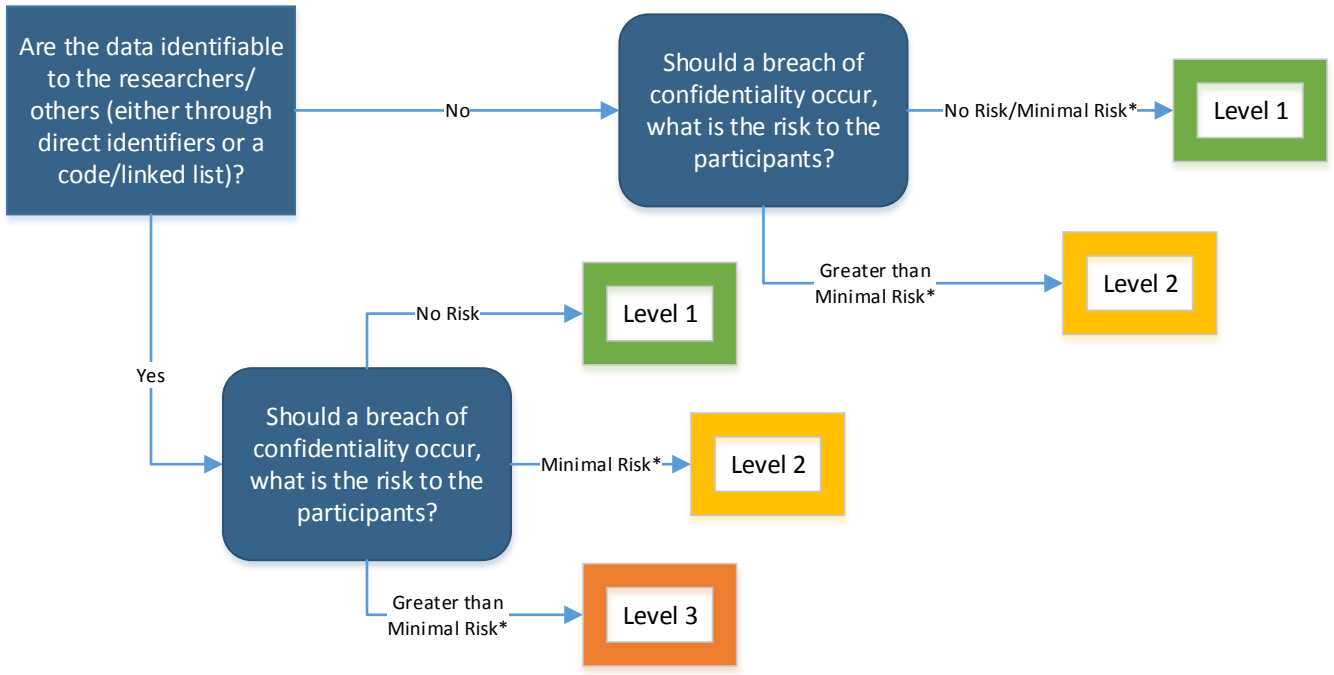
Determining Your Data Security Level

Oregon State University

Human Research Protection Program
Institutional Review Board
Office of Research Integrity
Phone: 541-737-8008
Email: IRB@oregonstate.edu
Website: oregonstate.edu/research/irb



Level 1 requirements:
Information should be shared and stored in a manner that provides access only to authorized individuals. If information is stored on a computer, the system should have fully patched operating systems and applications, and current antivirus software with current virus definitions. Information may be stored in cloud based servers.

*Minimal risk means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.
Examples per Risk Levels:

Greater than minimal risk: A study involving interviews with users of illegal drugs.
Minimal risk*: Interviews and observations of families experiencing food insecurity.
No risk: Surveys of personal opinion about trails available for hikers.

For more information, see the Data Security Guidance on the OSU IRB Website

Level 2 Requirements:
Information should be shared and stored in a manner that provides access only to authorized individuals. Data may not be disclosed to additional parties without prior IRB approval specifically authorizing the disclosure. If information is stored on a computer, the system should have fully patched operating systems and applications, and current antivirus software with current virus definitions. Information may be stored on approved cloud servers. The data security plan must be reviewed by the Information Security Office if the data security category is level 2 and the data is stored in a cloud-based server, unless the server is Qualtrics or OSU Google Drive. A plan for routine back-ups must be in place.

Level 3 Requirements:
Information should be shared and stored in a manner that provides access only to authorized individuals. Data may not be disclosed to additional parties without prior IRB approval specifically authorizing the disclosure. If information is stored on a computer, the system should have fully patched operating systems and applications, and current antivirus software with current virus definitions. When feasible, information should be stored in a local system of record (e.g., local server, approved cloud). All mobile computer systems or portable storage media must be encrypted with at least the 256-bit encryption common in operating systems and encoding devices sold in the United States. If the data is coded, and there is a linked list of codes and identifiers, this list should be stored separately from all coded data. Identifiable information should not be stored on student researchers' computers after the study has ended. Data security plans for systems storing Level 3 data must be reviewed by the Information Security Office. Computers must have host-based firewalls enabled in addition to being behind a networked firewall context. A plan for routine back-ups of all data must be in place, with the appropriate security mechanisms for that data, including encryption and physical security addressed.