Human Subjects Protections Guidelines for XR Research

XR is a powerful and flexible research tool in numerous disciplines. To continue productive research programs and support progress in innovation, practical steps can be taken to bolster human subjects protections and establish research guidelines that are applicable in both Social/Behavioral and Biomedical review processes.

The following checklist is intended to call attention to areas of additional levels of review for human subjects protections in XR research. The first goal is transparency in the collection, use, and storage of data. This will provide committees with the knowledge to evaluate the privacy risks to the participants. The second goal is to inform the participant of the planned and potential use of the data and provide choice on levels of consent. The third goal is ensure the safety of participants through research team empirical risk assessment and mitigation as well as relevant supplemental training beyond basic Human Subjects Research certification.

Review Criteria: Human Subjects Protections

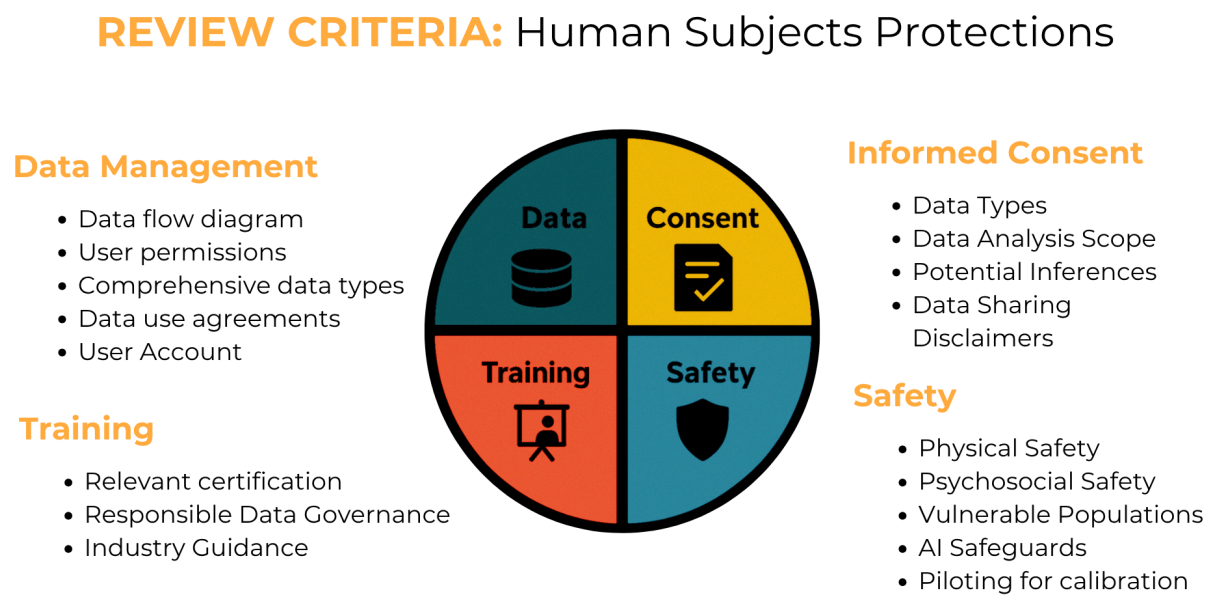

Figure 1: Review Criteria: Human Subjects Protections within categories of: Data; Consent; Training; and Safety.

Julia A Scott, PhD, Director of Brain and Memory Care Lab, Bioengineering, Santa Clara University; Council Lead, MedXRSI; Bhanujeet Chaudhary, Chief of Staff, XRSI; Aryan Bagade, MS Computer Science and Engineering, Santa Clara University
Originally presented at PRIM&R 2024 Annual Meeting

Data Management

- Data flow diagram
  A data flow diagram illustrate the data management plan and explicitly identifies how data moves through complex systems
- User permissions
  Limiting permissions to types of data within a research team with greater granularity than “de-identified” datasets
- Comprehensive data types
  Report all data types collected inclusive of intended, unintentional, and accidental
- Third-party data use agreements
  Include data use agreements of hardware devices and software applications used in the study
- User Accounts
  Provide justification for participant obligation to create user accounts with their personal identity

Informed Consent

- Data Types
  List categories of data collected in lay terms
- Data Analysis Scope
  Describe both the intended use of study data and future use
- Potential Inferences
  Identify risks in inferences related to personal and sensitive data, including any inference made by automated decision making systems/AI models
- Data Sharing
  Name which data types and metadata plans to be shared
- Disclaimers
  Highlight groups that may be at greater safety risk, in addition to exclusion criteria

Safety

- Physical Safety
  Identify environmental and personal safety measures implemented
- Psychosocial Safety
  Describe how psychological risks are accounted for and mitigated
- Vulnerable Populations
  Justify inclusion of vulnerable groups, especially those with mental health conditions
- AI Safeguards
  Determine whether participant is a data donor to AI models, Describe potential for user manipulation by AI, and identify the boundary conditions of generative AI

- Piloting for calibration
  Submit pilot study data that calibrating the content and intensity of the user experience in the study

Training

- Relevant certification
  Submit supplemental training for technology used
- XRSI Responsible Data Governance
  Consult industry standard for data management
- Industry Guidance
  Refer to domain specific guidance on best practices

Resources

Role	Organization
Developer	XRSI
Trials	VR-CORE
Medical	FDA resources for XR
Engineering	IEEE Standards XR
Psychology	APA's Mental Health Technology Advisory Committee
Ethics	XR Guild Library
Policy	XRA

Comparison of Risk Categories

The inputs from the workshop respondents were mapped to the review criteria in the suggested guidance and ranked based on the frequency of mention and the severity of concern (Table 1). Data privacy and user safety experts (Expert) evaluated the review criteria for each case study as a compartor. There were many areas of alignment between the research compliance officers (Learners) and Expert's assessments. Differences in risk assessment associated with AI and XR were evident, which were

more associated with depth of technical knowledge rather than differences in policy interpretation. In some areas, Learners overestimated safety risks (e.g. AI safeguards in Haptics). Then on other dimensions, Learners overlooked relevant mitigation strategies (e.g. Industry guidance in Biodata). The greatest discordance was in Data Management across all case studies.

Table 1. Review criteria for study protocols and sample rankings of level of relevance in broad study types by Expert and Learner assessments.

Review Criteria	Biodata	Haptics	Motion Tracking
Data Management			
Data Flow Diagram	HIGH	LOW	HIGH
User Permissions	MED	LOW	MED
Comprehensive Data Types	HIGH	LOW	HIGH
Third-party Data Use Agreements	MED	LOW	HIGH
User Accounts	LOW	NA	MED
Informed Consent			
Data Types	HIGH	LOW	HIGH
Data Analysis Scope	MED	MED	HIGH
Potential Inferences	HIGH	LOW	HIGH
Data Sharing	MED	LOW	MED
Disclaimers	HIGH	HIGH	HIGH
Safety			
Physical Safety	MED	HIGH	LOW
Psychosocial Safety	HIGH	MED	LOW
Vulnerable Populations	HIGH	HIGH	LOW
AI Safeguards	MED	NA	HIGH
Piloting for Calibration	HIGH	HIGH	LOW
Training			
Relevant Certification	MED	HIGH	NA
Responsible Data Governance	MED	LOW	HIGH
Industry Guidance	HIGH	HIGH	LOW