Guidance for Human Subjects Researchers:

Selecting Appropriate Platforms for Data Collection and Storage

Texas A&M University-Texarkana IRB

When conducting research, researchers must address two distinct aspects of data protection: protection by researchers and protection by the platforms used for data collection and storage. For detailed information on safeguarding participant confidentiality and privacy, researchers should refer to the CITI training modules on human subject protection available through the University. This guidance focuses on selecting platforms that protect participant data and align with the research's risk level, including minimal-risk research and higher-risk research requiring HIPAA or FERPA compliance.

Important Note on Google Forms

Google Forms is not approved for research purposes due to insufficient transparency regarding data handling and storage practices. While Google provides encryption, concerns remain about how data is processed and managed in the cloud. Any protocols submitted to the IRB using Google Forms will be returned to the researcher for revision. Researchers should prioritize approved platforms to ensure ethical and compliant data collection.

Researcher Access to Approved Platforms through the University

The University provides access to Qualtrics, a secure platform that meets institutional requirements for data protection. It is recommended for all research projects, regardless of risk level.

Accessing Qualtrics: Researchers can access the University's Qualtrics site through the TAMUT portal, located in the Digital Backpack. Qualtrics includes options to create a login page for remote internet access, allowing researchers to manage surveys securely and conveniently.

Alternative Platforms for Data Collection and Storage Platforms for IRB-Exempt or Minimal-Risk Research

For human subjects research involving no (IRB-exempt) or minimal risk, as determined by the IRB (e.g., anonymous surveys or non-sensitive data storage), the following platforms are generally appropriate:

- **Qualtrics:** Fully supported by the University and recommended for most research.
- **SurveyMonkey:** Offers strong data protection features, suitable for minimal-risk research.
- **REDCap:** Secure web-based application widely used in research settings.
- **Alchemer (formerly SurveyGizmo):** Provides customizable forms with robust security.
- **Formstack:** Offers secure, user-friendly forms with data protection features.
- **FormAssembly:** Customizable forms with strong security measures for minimal-risk research**.**

Platforms for HIPAA- or FERPA-Compliant Research

Certain research projects may require platforms that meet Health Insurance Portability and Accountability Act (HIPAA) or Family Educational Rights and Privacy Act (FERPA) compliance standards. Such projects may involve expedited or full board review depending on the research's risk level.

- HIPAA Compliance is required for research involving Protected Health Information (PHI). Entities that must meet HIPAA requirements include healthcare providers, health plans, healthcare clearinghouses, and their business associates.
- FERPA Compliance is required for research using Personally Identifiable Information (PII) from student educational records maintained by educational institutions.

For such projects, researchers may consider the following platforms:

- **Qualtrics:** Fully compliant when configured appropriately.
- **REDCap:** Designed for secure, compliant data collection.
- **Alchemer:** Offers compliance options for HIPAA and FERPA with proper configurations.
- **Formstack:** Provides HIPAA-compliant forms and secure data storage.
- **FormAssembly:** Offers HIPAA and FERPA compliance with customizable, secure forms.
- **Jotform:** Can be configured to meet HIPAA compliance requirements.

Data Storage Considerations for All Research

Researchers must ensure that platforms used for storing data (even beyond surveys) meet the following requirements:

- **Data Security:** Encryption during data transmission and storage (e.g., SSL/TLS protocols).
- **Access Control:** Use of multi-factor authentication and role-based permissions.
- **Backup and Recovery:** Regular data backups and disaster recovery plans.
- **Compliance Documentation:** Clear evidence of compliance with relevant standards (HIPAA, FERPA, or other applicable laws).

Documentation Requirements for Non-Qualtrics Platforms

Researchers choosing a platform other than the TAMU-T approved Qualtrics must include the following documentation in their IRB application appendices:

1. Platform Name and Version: Clearly identify the software being used.
2. HIPAA and/or FERPA Compliance Verification:
    - How to Verify Compliance: Researchers can check the platform's official website, compliance certifications, or request documentation directly from the provider.
    - Specific Compliance Items to Include:
        - Evidence of encryption standards (e.g., SSL/TLS protocols).

- Details on data storage and handling (e.g., physical server locations, backup protocols).
- Statements or certifications of HIPAA or FERPA compliance.
- Information on access controls, such as multi-factor authentication.

Key Points for Researchers

- Minimal-Risk Research: Use platforms with robust data security features, such as Qualtrics, SurveyMonkey, REDCap, Alchemer, Formstack, or FormAssembly.
- Higher-Risk Research: Use a platform explicitly designed for HIPAA and/or FERPA compliance and submit required documentation to the IRB.
- Data Storage: Ensure all platforms used for data storage meet high security standards, regardless of research type.
- University Support: Qualtrics is the preferred platform for all research and is accessible through the TAMUT portal.
- Google Forms is not allowed: Due to privacy concerns, Google Forms is not suitable for any research project.

By following these guidelines, researchers can ensure the protection of participant data, maintain compliance with regulatory requirements, and uphold ethical research standards. For additional support, contact IRB@tamut.edu.