Institutional Review Board Electronic Data Management Policy

Purpose

Information in electronic formats presents specific challenges to researchers and administrators when planning for methods of collecting, storing, transmitting, controlling access to, and disposing of information that adequately preserves the confidentiality, integrity, and availability of the data.

Keep in mind that electronic records can be quickly and readily replicated and circulated without any obvious indications that this has happened. Electronic records can be easily modified, therefore consider controls that help maintain the integrity of the data.

Computer and Internet-based methods of collecting, storing, utilizing, and transmitting data in research involving human participants are developing at a rapid rate. As these new methods become more widespread in social and behavioral research, they present new challenges to the protection of research subjects.

Research protocols utilizing digital instruments must address the same risks (e.g., violation of privacy, legal risks, and psychosocial stress) and provide the same level of protection as any other types of research involving human participants. All studies, including those using digital technologies, must (a) ensure that the procedures fulfill the principles of voluntary participation and informed consent, (b) maintain the confidentiality of information obtained from or about human participants, and (c) adequately address possible risks to participants including psychosocial stress and related risks.

The IRB considers the defense-in-depth security measures the best course of action to ensure the maintenance of the confidentiality of participant data. Password access when combined with encryption, better guarantees that even if the media fall into the wrong hands, the data are less likely to be retrieved. Physical access controls should not be overlooked when planning for adequate security. Physical controls (such as locks) when combined with technical controls (such as passwords and encryption) provide for a greater depth of defense.

Scope

The IRB intends for the following information to address the key concepts of data confidentiality, integrity, and availability. Unless noted otherwise this information pertains to all projects subject to the review of the University at Albany Institutional Review Board (IRB), whether they are of minimal risk or not. Any deviation from these requirements must be scientifically justified and approved by the IRB. In determining the adequacy of certain survey programs, data collection and storage methods, and informed consent procedures for the protection of human participants, the IRB will assess whether proposed research is minimal risk or more than minimal risk. For each study reviewed by the IRB additional requirements may be imposed depending on the level of risk the study imposes on the participants and the specific circumstances of the study.
Recruitment

- Computer and Internet-based procedures for advertising and recruiting potential study participants (e.g., internet advertising, e-mail solicitation, banner ads) must follow the IRB guidelines for recruitment that apply to any traditional media, such as newspapers and bulletin boards.
- The IRB does not consider e-mail addresses publicly available unless they are on a publicly accessible server/website that does not require the user to login.

Encryption

Data encryption transforms plain text files into a format that prevents unauthorized users from opening the files and reading the contents. There are two types of encryption that should be considered: data at rest, and data in transit. The former protects stored data while the latter protects data as they are being transmitted between parties over a public network. Unless otherwise specified by the IRB, it is recommended that the highest level of data encryption be used, within the limits of availability and feasibility.

Data at Rest

Data at rest refers to all data stored on electronic media. Encryption for data at rest is provided by some operating systems (e.g., Windows Encrypted File Services), or third party applications, both commercial (PGP) and open source (Truecrypt). Data may be encrypted at the system level (full disk encryption), or the individual folder or file level. The encryption of data at rest may be deemed necessary by the IRB depending on the circumstances of the study and the data being collected.

Data in Transit

Data in transit is data that are actively being transmitted over a network from one location to another. The most common forms of encryption for data in transit are Secure Socket Layer/Transport Layer Security (SSL/TLS). These require the use of certificates issued by certificate authorities. SSL/TLS are generally used in circumstances where a client computer is talking to a server. A common example is a web browser used to interact with an on-line commercial or banking server. Using the SSL/TLS protocol helps ensure that any data intercepted during transmission cannot be viewed and modified, preventing individual responses from being traced back to an individual respondent. This may require that the participants be encouraged or required to use a specific type or version of browser software. Researchers are cautioned that encryption standards vary from country to country and that there are legal restrictions regarding the export of certain encryption software outside of US boundaries.

Spam

Unsolicited e-mail messages to multiple users are prohibited unless explicitly approved by the appropriate authority. All messages must show accurately from where and from whom the message originated. The IRB may consider waiving this requirement under specific circumstances that are assessed on an individual case basis.
Authentication

Authentication (proper qualification and/or identification of respondents) is a major challenge in computer and Internet-based research and one that threatens the integrity of research samples and the validity of research results. Depending on the level of risk the study imposes on the participants and the specific circumstances of the study, researchers may be advised to take steps to authenticate respondents. For example, investigators can provide each study participant (in person or by U.S. Postal Service mail) with a Personal Identification Number (PIN) to be used for authentication in subsequent computer and Internet-based data collection.

Informed Consent

• All studies approved by the IRB to use computer and Internet-based survey instruments must include the following statement in the informed consent form:

  This project has been approved by the University at Albany Institutional Review Board. Approval of this project only signifies that the procedures adequately protect the rights and welfare of the participants. Note that absolute confidentiality cannot be guaranteed due to the limited protections of Internet access.

• At this time, a waiver of documented signed informed consent must be requested if a signature affixed by hand is not used. Digital and electronic signatures are an evolving technology.¹ Their use for research projects shall be determined on a case-by-case basis. The IRB will consider the risk level, data being collected and the circumstances of the project when considering whether digital or electronic signatures may be used as evidence of signed informed consent. Furthermore, guidance from the federal Office for Human Research Protections (OHRP) on this issue may be found on-line at: http://answers.hhs.gov/ohrp/questions/7260

Participation by Minors

• Researchers are subject to the Children’s Online Privacy Protection Act of 1998 when subjects are (or include) minors under the age of 13.² Researchers are prohibited from collecting personal information from a child without posting notices about how the information will be used and without getting written parental permission. For minimal risk research, written permission may be obtained via postal mail or fax. If the research is more than minimal risk, parental permission should be obtained in a face-to-face meeting.

• For research that excludes minor participants, the IRB may ask the researcher to describe the procedures to be employed to authenticate that the participants are adults. Some options are using Internet monitoring software or using Adult Check systems that can screen out minors.

¹ The IRB defines electronic signatures as computer data compilations of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual’s handwritten signature. Add digital signatures are defined as an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

• Depending on the level of risk, as determined by the IRB, and the circumstances of the study, the IRB may deem additional appropriate measures to be taken to reasonably ensure protection of minors and any collected personal information.

Collection

• Any investigator that collects regulated data – defined as any data elements or data collections subject to regulatory controls – must disclose the collection of such data to the IRB and the Information Security Officer (ISO). Additionally, researchers are responsible for:
  a. minimizing the use of SSN or other forms of personal identification;
  b. maintaining an up-to-date inventory of SSN databases and datasets, and other repositories of identifiers;
  c. documenting security controls and risk remediation and communicating these to the IRB and ISO; and
  d. If such data are collected about University at Albany faculty, staff or students, the researcher must comply with the University policy on “Protection and Use of Faculty, Staff and Student Identifiers”.

• Researchers must submit Supplemental Form 16 with their protocol when digital data collection instruments (e.g., on-line surveys or e-mail) are intended to be used in the project.

• Data collected on servers from participants over computer networks must be transmitted in encrypted format via a secure server using the SSL/TLS protocol.

• Regulated data that are collected over e-mail from participants must be transmitted using a shared key procedure. This procedure is outlined below in the Transmission section.

• Depending on the exact data being collected and the circumstances of the study, the IRB and ISO will determine the appropriate measures which must be taken to reasonably ensure confidentiality of the data.

Storage

• Data stored in relation to IRB approved studies determined to constitute more than minimal risk to participants must be stored on encrypted drives using PGP or equivalent protection (as determined by the IRB) in a secure location and in a manner that ensures only authorized access to the data, and that no unauthorized changes can be made to the data.

• Data stored in relation to IRB approved studies determined to constitute minimal risk to participants must be stored in a secure location or manner that ensures only authorized access to the data, and that no unauthorized changes can be made to the data.

• Any requirements of study sponsors shall not be construed to require less security than indicated in this or any other University data management policy.

• Where feasible, consideration should be given to backups in the event of loss or damage to the primary data collection.

---

3 Examples of regulated data include education records (FERPA), personal health information (HIPAA), Social Security numbers (SSN) (as outlined in NYS ISBN Law, NYS Labor Law, NYS Public Officers Law), and certain financial records (FTC Red Flag Rules, Gramm Leach Bliley). Penalties for failing to comply with regulatory requirements can result in severe financial and operational sanctions (e.g., loss of federal education aid).
• The physical storage location(s) should be reasonably secure against theft and loss due to fire, flood, electrical surges, and other forms of physical damage.

• Personally identifiable information (e.g., IP addresses) must be kept separate from the data and in accord with the University’s policy “Protection and Use of Faculty, Staff and Student Identifiers”.

• Use of external vendors for data storage and transfer (i.e., cloud storage) is permitted subject to final IRB approval. For data related to studies determined to be more than minimal risk to participants, the data must be stored encrypted on secure servers, using the SSL/TLS protocol while in transit, and in a secure location in a manner that assures only authorized access to the data, and that no unauthorized changes can be made to the data.

Transmission

• As discussed in the Encryption and Collection sections, unless data are encrypted in storage (at Rest) or during transmission (in Transit), there is a risk that participants’ information may be exposed if unauthorized individuals gain access to the data. The solutions to the problems of securing Data at Rest or in Transit are full disk encryption and the use of SSL/TLS. Sharing collections or subsets of collections of data with colleagues or research partners poses a separate problem, particularly when e-mail is used to share the information. In these cases, encryption is also an effective and acceptable solution to protecting confidentiality, but requires a different set of software tools. Sending encrypted messages to authorized colleagues requires the sharing of encryption keys. There are many products designed to facilitate e-mail encryption. Several links to compilations of these products are provided below. They all require two fundamental operations: 1. the generation of a public/private key pair; and 2. the publication of the user’s public key to a key server such as pgp.mit.edu. Specific instructions on how to perform these operations accompany each of the products. Email Encryption Software

  http://www.openpgp.org/
  http://www.softsea.com/software/Email-Encryption.html

A General Discussion of Public Key Encryption

http://en.wikipedia.org/wiki/Public-key_cryptography

• The IRB will make the final determination regarding the appropriate level of security required when transmitting data between colleagues or research partners depending on the level of risk the study imposes on the participants and the specific circumstances of the study.

Access Control

• A unique password or passphrase must be implemented at the user account level for each researcher and for all computers containing data related to research, subject to IRB approval. In general, longer passphrases (greater than 12 characters) are more secure and easier to remember than short, complex passwords.

• Computers containing data related to research subject to IRB approval must be kept in a location physically secured with locking mechanisms. Such locations should be on campus whenever possible. Locks may utilize a physical key, key card, or keypad.
Data Retention, Destruction and Disposal

- All data, whether electronic or hardcopy, must be retained a minimum of three years after the end of the research project per federal regulations. Pursuant to guidelines issued by the Research Foundation and Office for Pre-Award and Compliance Services Record Retention policy, research records must be kept for six years beyond the term of the grant. These data must be continued to be kept in a secure location with appropriate controls for data at rest for the duration of the retention period.
- After the required retention period, data should be destroyed. Data destruction should be accomplished by physical destruction of the media containing the data, or by using National Institute of Standards and Technology’s recommended methods and tools for media sanitization (See “Special Publication 800-88: Guidelines for Media Sanitization”).

Server Administration

- Researchers who manage, own or operate their own server systems on the University’s network must comply with the University’s “Standards for Connecting Servers to the University Network.”
- Investigators that contract with an external vendor (e.g., Surveymonkey.com, Dropbox.com) must provide evidence that the vendor complies with the following criteria:
  - the server is administered by a professionally trained person with expertise in computer and internet security;
  - access to the server is limited to key project personnel and is configured to minimize the possibility of external access to the server data;
  - data is transferred and encrypted using SSL/TLS protocol;
  - there are frequent, regularly scheduled security audits of the server; and
  - the provider is capable of meeting any other requirements the IRB may deem necessary for the protection of identifiable private information of human subjects.

Adverse Incident Reporting

- Breaches of subject confidentially should be reported to the IRB immediately and in conformance with the IRB’s reporting requirements for adverse events and the University's Information Security Incident Response protocol. Reports must include:
  - the date and time of the incident;
  - the nature of the information that was compromised;
  - confirmation that the breached system has been isolated, secured, and not modified for forensic purposes;
  - a plan for notifying affected individuals that a confidentiality breach has occurred; and a corrective action plan.