University of Colorado Boulder

Office of Research Integrity
Institutional Review Board
3100 Marine Street | ARC Room A15
Boulder, CO 80309
irbadmin@colorado.edu | (303) 735 - 3702

Guidance Document: Data Security

Background

The criteria for approval outlined in the federal regulations governing human subjects research include "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data." Likewise, the CU Office of Information Security (CU-OIS) recognizes the need to protect data and has issued guidance informed by the National Institute of Standards and Technology on the appropriate system level securities that should be implemented in order to enhance confidentiality, integrity and availability of data.

The following guidance represents the IRB Office's perspectives on management and security of data involving human subjects. This guidance is not meant to be viewed as CU Boulder's full policy regarding data security classification and management, which is managed by CU-OIS. Please contact CU-OIS at InfoSec@colorado.edu for more information about CU's Process for Data Classification and System Security Categorization or if you have questions about how to implement any of the data security procedures outlined below.

Generally, OIS views data security risks in two categories: those dealing with the confidentiality requirements for the data, and those dealing with the possible harm, or "impact" posed by the data. The final data security classification will be made based on where the data fall in these categories both individually and in combination (see the Data Security Matrix). Note that these definitions do not directly relate to the Minimal/Greater than Minimal Risk determination that will be made by the IRB.

Definitions

Confidentiality Requirements		
Highly Confidential Information:	**Confidential Information:**	**Public Information:**
Data that require protection under laws, regulations, contracts, relevant legal agreements and/or require the institution to provide notification of unauthorized disclosure/security incidents to affected individuals or government agencies. This information is only for the "eyes of authorized individuals" in any form including paper or electronic.	Identifiable information provided to or obtained by investigators, in which the person to whom the information pertains has provided the data with an expectation that confidentiality would be maintained. This includes both data collected specifically for research purposes (i.e., resulting from an interaction or intervention with the subject) and data created for non-research purposes and accessed or collected by an investigator for research. This category includes data elements not usually disclosed to the public but that are less sensitive than Highly Confidential data. These data may be released if subject to a Colorado Open Records Act (CORA) request.	Information that is collected in contexts where no expectation of privacy exists. OR Data that are obtained, collected or maintained in such a manner that they cannot be linked directly or indirectly to an individual subject (i.e., are "anonymous"). This does not include data accessed or recorded in an identifiable format and later de-identified, prior to de-identification (unless public as described above) nor any data in which a linking document exists (i.e., coded data). This category includes any information that is publically available and accessible without authentication, such as information that is freely available through print material.

University of Colorado Boulder

Office of Research Integrity
Institutional Review Board
3100 Marine Street | ARC Room A15
Boulder, CO 80309
irbadmin@colorado.edu | (303) 735 - 3702

Confidentiality Requirements		
Highly Confidential Information:	**Confidential Information:**	**Public Information:**
Examples include: • Protected Health Information (PHI) as defined in HIPAA regulations • Social Security Numbers • Financial Aid information • Legal Presence • Visa Status and/or Citizenship • Data collected under a Certificate of Confidentiality from NIH	Examples include: • Health related information not subject to HIPAA regulation • Personnel records, benefits, salaries and employment applications • Student Data Protected under FERPA • Admission applications • GPA • Identifiers such as gender, birthdate, race, ethnicity • Affiliation or member of a stigmatized group (i.e., KKK, gangs, IRA) • Religious affiliation	Examples include: • University directory information • Observations of public behavior • Data collected from public websites, blogs, chatrooms, etc. (Note expectations of privacy in online settings vary and should be carefully considered. Websites requiring a specific invitation or approval to view information should not generally be considered public.) • Information about individuals gleaned from publications (news articles, etc.)

Subject Impact		
High Impact Data:	Moderate Impact Data:	Low Impact Data:
If a breach of confidentiality were to occur, the information could cause harm to an individual. Risks may include criminal or civil liability, psychological harm or other injury, loss of insurability or employability or social harm to an individual or group.	In the event that individually identifiable data are disclosed, there is a reasonable expectation that an individual may suffer reputational harm or embarrassment.	Accidental release of the information would result in no or insignificant harm to the individual.

Security Requirement Determinations

Security requirement determinations are made in the context of the broader environment. When making a security requirement determination it is vital to consider the potential impact to subjects and how identifiable the data are. For example, a research subject may disclose highly confidential information, but if the data are anonymous or de-identified it may be subject to less intensive security requirements.

Data Security Matrix			
	Low Impact	***Moderate Impact***	***High Impact***
Public Information	Level 1	Level 1	Level 3*
Confidential Information	Level 2	Level 2	Level 3
Highly Confidential Information	Level 3	Level 3	Level 3

**A level 3 classification requires Office of Information Security (OIS) Review*

Level 1: Data are public or anonymous; or are identifiable and the subject has provided consent to make their data publically available; or data are identifiable but appropriate security mechanisms are in place to safeguard the data even though the data presents no risk to the subject. Information of this type are stored on password protected computers that have a fully patched operating system and applications, current antivirus software with current virus definitions. Data may be stored in a cloud-based server. Access to data is limited to authorized individuals.

Office of Research Integrity
Institutional Review Board
3100 Marine Street | ARC Room A15
Boulder, CO 80309
irbadmin@colorado.edu | (303) 735 - 3702

Level 2: Data are individually identifiable and may present minimal risk of harm if disclosed outside of the research; or there is an expectation of privacy or confidentiality. Data of this type should be accessed through authenticated mediums on a need to know basis. Only electronic mediums and services (emails, file shares, etc.) approved by the institution are used to transmit/store data. Computers used to store data have the latest anti-virus, security updates installed and reside on networks that have appropriate security controls in-place (firewalls, monitoring, logging). Information may be stored in approved cloud servers.

Level 3: Data are individually identifiable and would place the subject at risk of harm if disclosed OR are explicitly protected by legal requirements or regulation. These data are only for "eyes of authorized individuals" in any form, including paper or electronic. This information is prohibited from being transmitted or stored without encryption, handled on networks or systems without appropriate firewall, monitoring, logging, patching, anti-malware and related security controls. A plan for data retention of level 3 data is required. ***Studies for which data falls into level 3 must have their data management plan approved by the Office of Information Security prior to IRB submission.***

References

National Institute of Standards and Technology. (2015, May 19). *Publications: NIST.* Retrieved from NIST Web site: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

Oregon State University. (2015, May 12). *Data Security: Institutional Review Board.* Retrieved from OSU Institutional Review Board web site: http://research.oregonstate.edu/irb/policies-and-guidance-investigators/guidance/data-security

University of Colorado. (2013). *University of Colorado Process for Data Classification and System Security Categorization.* Office for Information Security.