|  |  |
| --- | --- |
| Logo | **GUIDANCE Data Security Protections** |
|  | |
|  | |

**This document is modelled on the Harvard University Information Security Policy for research data.**

| **PURPOSE** |
| --- |
| **Purpose**. This document describes the types of data security protections that the UW IRB generally expects researchers to provide for human subjects data, according to the possibility and type of harm associated with a breach of the data. These expectations are in addition to other University requirements that may apply, such as UW Medicine requirements for Protected Health Information (<http://depts.washington.edu/comply/policies-procedures/>) and general University requirements (<https://ciso.uw.edu/>).   * This document is meant to assist researchers in identifying appropriate protections. If an expectation described here does not make sense for the particular circumstances of a study (for example, some international settings), researchers may inform the IRB and provide the rationale as well as what protections will be available.   **Resources**. Researchers are encouraged to consult with their department IT support, as needed. Many of the protections described here are already part of UW IT-supported servers and networks, and would not require any additional work or resources from researchers. Additional information and resources are available at:   * <https://itconnect.uw.edu/security/securing-computer/> * <https://depts.washington.edu/uwmedsec/restricted/guidance/encryption/> (UW netID protected content)   **Reporting breaches and loss**. Reporting suspected breaches or loss of data as soon as possible to all relevant offices is an important data security protection for all research. These must be reported as soon as possible to the IRB, and (for protected health information) to UW Medicine, and (for certain types of information critical to identify theft or financial fraud), the UW CISO’s office. |

|  |  |
| --- | --- |
| **1. DESCRIPTION OF RISK LEVELS FOR UNPROTECTED DATA** | |
| **Level 1: Very low risk of harm if disclosed.** | |
| **Description** | These data have little or no sensitivity. Disclosure of these data would have very little or no risk of physical, psychological, social, economic, legal, or educational advancement harm to the subjects. |
| **Examples** | * De-identified, anonymous, or publicly available data * Data for which subjects have consented to allow public access (e.g., a museum archive) * Opinions of individuals about non-sensitive issues, or performance on non-sensitive tasks |
| **Level 2: Some risk of minor harm to individuals if disclosed** | |
| **Description** | These data have relatively little sensitivity except possibly short-term embarrassment or psychological discomfort if the data were disclosed. |
| **Examples** | * Performance of individuals on non-sensitive tasks in a competitive situation * Genetic information about individuals’ metabolism of medical drugs such as statins |
| **Level 3: Could cause risk of material harm to individuals if disclosed.** | |
| **Description** | These data could result in harm that can have genuine impact, but the magnitude and/or duration are generally not serious, long-lasting, and/or irreversible. |
| **Examples** | * Non-sensitive Personal Health Information |
| **Level 4: Would likely cause serious harm to individuals if disclosed** | |
| **Description** | These data could result in serious harm. |
| **Examples** | * Sensitive Personal Health Information, such as the history of cancer or other significant conditions which could (for example) affect employability or insurability |
| **Level 5: Extremely sensitive; could cause severe harm to individuals if disclosed** | |
| **Description** | These data could result in serious and long-lasting harm. |
| **Examples** | * Information about subjects’ illegal behavior * Very sensitive Personal Health Information, such as the diagnosis of HIV/AIDS in some cultures or a diagnosis of leprosy |

|  |
| --- |
| **2. EXPECTED DATA SECURITY PROTECTIONS BY RISK LEVEL – Level 2 through Level 5** |
| **Level 1**: No specific protections are required above and beyond standard University expectations. However, the UW IRB strongly encourages the adoption of some or all of the data security protections described for Level 2. |

|  |  |  |  |
| --- | --- | --- | --- |
| **USERS: The individuals who have access to, or will use, the data.** | | | |
| **Requirements** | | **Description** | **Applies to** |
| U1 | Limit access | Limit the access to appropriate users, except when the data are intentionally made public. Limitation is provided through the use of passwords or other access credentials or mechanisms, depending upon the nature and location of the data. | L2 – L5 |
| U2 | No shared passwords | Users’ passwords and other access credentials should not be shared. | L2 – L5 |
| U3 | Protection of passwords | Passwords and other access credentials should be protected.  *For example, use a password management application such as 1Password, LastPass, KeePass or iCloud Keychain that generates stores and protects long, random, unique passwords.* | L2 – L5 |
| U4 | Strong passwords | Passwords should be of sufficient length and complexity to reasonably protect them from being guessed by humans or computers. | L2 – L5 |
| U5 | Different passwords | Different passwords should be used for UW and non-UW access. | L2 – L5 |
| U6 | Changing passwords | Passwords should be changed periodically. | L2 – L5 |
| U7 | Compromised passwords | Passwords should be changed immediately if there is suspicion of compromise. | L2 – L5 |
| U8 | Report loss of data | Any actual or suspected loss, theft, or improper use of (or access to) the data must be reported immediately to the IRB and any other appropriate entities (such as the UW Medicine Privacy Office). | L2 – L5 |
| U9 | Data storage policy | Researchers should separate subject identifiers from the data, using a “key” or code to link identifiers to the data. The link between the key/code and the identifiers should be placed in a separate password protected file that is stored in a different physical location than the data. | L3 – L5 |
| U10 | Documentation of access | A written process is established and followed for documenting who has access to the data.  This applies to all individuals, whether or not they are members of the study team. | L3 - L5 |
| U11 | Data disposal | Destroy, return, or de-identify data if the data are no longer needed and the applicable records retention period has ended. The method should be appropriate to the risk and sensitivity of the information. | L3 - L5 |
| U12 | Authorization process | A written process is established and followed for requesting and approving access to the data, including:   * The criteria used for granting access * Identification of who is responsible for approving access * A mechanism for revocation of an individual’s access, because there is no longer a need for access or access has been inappropriately used or protected   This applies to all individuals, whether or not they are members of the study team. | L4, L5 |
| U13 | Confidentiality and security training | A written process is established and followed for ensuring and documenting that appropriate training about confidentiality and data security has been provided to individuals who will have ongoing access to the data.  *CITI human subjects training is not sufficient for meeting this requirement.* | L4, L5 |
| U14 | Authorized uses | There is a written data use agreement that defines the authorized uses of the data by anyone outside of the study team who is given access to the data. | L4, L5 |
| U15 | Certificate of Confidentiality | **ENCOURAGED but not required unless the IRB explicitly requires it for the specific study**. Apply for a federal Certificate of Confidentiality or Privacy Certificate, to protect against disclosure of the data in response to a subpoena or other legal process. | L4, L5 |
| U16 | Monitoring of these user requirements | A written process is established and followed for monitoring the fulfillment of the user requirements. | L5 |

|  |  |  |  |
| --- | --- | --- | --- |
| **DEVICES: User devices (including portable devices but not servers) on which data are collected, processed, and/or stored. Examples: desktop computer; laptop computers; smart phones; USB or flash drives; iPads; laptops; tablet computers; DVDs.** | | | |
| **Requirements** | | **Description** | **Applies to** |
| D1 | Configure the device | Configure the device for secure operation, to limit access to the specific person or persons authorized to use the device. | L2 – L5 |
| D2 | Configure the applications | Configure the applications being used on the device, to protect the access and transfer of data. | L2 – L5 |
| D3 | Update the operating system and applications | Keep the operating system and applications up to date, by installing revisions, patches, and upgrades. | L2 – L5 |
| D4 | Protection against loss | Store or otherwise secure the device in a way that minimizes the possibility of loss or theft.  *Do not leave laptops and other mobile devices in your car.* | L2 – L5 |
| D5 | Device disposal | Before disposing of the device, the data stored on it must be de-identified, physically destroyed, over-written or wiped using a method that is appropriate to the risk and sensitivity of the data. | L3 – L5 |
| D6 | Portable devices | Portable devices cannot be used for storage of identifiable data except when specifically allowed by the IRB because of exceptional and well-justified circumstances. | L3 - L5 |
| D7 | Permanent storage | All data should be downloaded from local or portable devices to a secure server or service as soon as possible. | L3 - L5 |
| D8 | Encryption | The data must be encrypted.  *Encryption is a process that uses a mathematical algorithm (cipher) to transform information from a readable form into a form (ciphertext) that is unreadable by anyone that does not have the electronic key. Decryption is the reverse process. See some examples of methods at:*  [*https://depts.washington.edu/uwmedsec/restricted/guidance/encryption/*](https://depts.washington.edu/uwmedsec/restricted/guidance/encryption/%20) *(UW NetID required)* | L4, L5 |
| D9 | Device management & monitoring | A written process is established and followed for ensuring that:   * Devices are appropriately configured * Patches (and as appropriate, revisions) to operating systems and applications are installed * Devices have not been lost or stolen * Devices are being used appropriately | L4, L5 |

|  |  |  |  |
| --- | --- | --- | --- |
| **SERVERS / SERVICES: Computer servers or computing services on which data are collected and/stored, including file sharing or collaboration services. Examples: DropBox; cloud-based storage; email, or backup & recovery services, such as google docs; department servers; Mechanical Turk; Redcap; UW Catalyst.** | | | |
| **Requirements** | | **Description** | **Applies to** |
| S1 | Complex passwords\* | Servers and services that manage passwords must force the setting of a complex password:   * No common names or dictionary words * Use of uppercase/lowercase; number, and/or special character * Length requirements | L2 – L5 |
| S2 | Server communication\* | Communications between (1) servers or services and (2) client machines must be protected. | L2 – L5 |
| S3 | Server – application communication\* | Communications between servers or services must be protected. | L2 – L5 |
| S4 | Password change method\* | Mechanisms for users to set or change passwords must be secure. | L2 – L5 |
| S5 | Server operators\* | People responsible for the operation of servers must have the skills, experience, and/or training needed to implement these requirements. | L2 – L5 |
| S6 | Commercial services | Researchers are responsible for learning about the security protections for any commercial service they use, such as Mechanical Turk, file-sharing services, and cloud services. This includes selecting among options for appropriate configurations and protections. | L3 – L5 |
| S7 | Current patches\* | Operating systems and application patches are current. | L3 – L5 |
| S8 | Malware detection\* | The server or services run applicable malware detection software with up-to-date signature files. | L3 – L5 |
| S9 | No shared accounts\* | Server operators must not knowingly permit shared user account credentials. | L3 – L5 |
| S10 | Administrative functions\* | Administration functions on servers and applications must be logged. | L3 - L5 |
| S11 | Idle sessions\* | A mechanism must be used to force re-authentication to user accounts after an idle period. | L3 - L5 |
| S12 | Improper access\* | Servers must be protected from improper network-based access. | L3 – L5 |
| S13 | Logging access\* | User and administrator access to servers and applications must be logged. | L3 – L5 |
| S14 | Reporting breaches | Server and application operators must promptly inform the researchers (and through them, the IRB) of any suspected breaches. | L3 – L5 |
| S15 | Reviewing logs\* | The logs must be periodically reviewed for anomalous behavior. | L3 – L5 |
| S16 | Secure disposal\* | Secure overwriting of the data or physical destruction of the media are used to dispose of data that are no longer needed. | L3 – L5 |
| S17 | Password guessing | Servers or services must implement a mechanism that inhibits password guessing attacks on user accounts if the server or service does its own authentication. | L4, L5 |
| S18 | Server vulnerability | Server operators must take reasonable actions on a regular basis to ensure that their systems are not vulnerable to attack. | L4, L5 |
| S19 | Secure location | The server must be kept in a secure location and be subject to regular inventory to ensure that loss or theft is identified. | L4, L5 |
| S20 | Encryption | Data must be encrypted. | L5 |
| S21 | External access | The server or services must not be directly accessible from the Internet or from parts of the UW network where there are user computers, except when specifically allowed by the IRB because of exceptional and well-justified circumstances. | L5 |
| S22 | Protecting servers | Servers on the same subnet must be protected against attack from each other. | L5 |

*\*These requirements may be assumed to be met if the server or service is under the direct authority and control of UW IT, UW Medicine IT, or the Office of Research Information Services. Other requirements may also be met for specific servers but should be verified.*

|  |  |  |  |
| --- | --- | --- | --- |
| **PAPER & OTHER NON-DIGITAL RECORDS: Non-digital forms of data storage, including (for example): paper; non-digital film or tape recordings; non-digital drawings or artwork.** | | | |
| **Requirements** | | **Description** | **Applies to** |
| P1 | Limiting access | Access must be limited to those persons with valid reasons to access the records. | L2 – L5 |
| P2 | Protecting records | The records must be in a locked and secure location when not in active use. | L2 – L5 |
| P3 | Destruction of records | Destruction of records (after the end of the records retention schedule and if appropriate) must be accomplished by means that make it impossible to reconstruct the records. | L3 – L5 |
| P4 | Documentation of access | The names and roles of all individuals who have access to the data is documented and tracked over time.  *Be sure to consider non-research personnel such as administrative and custodial staff.* | L5 |
| P5 | Logging access | Access to the records for anything other than routine study operations should be logged. | L5 |

|  |  |  |  |
| --- | --- | --- | --- |
| **DATA TRANSMISSION: The methods by which data are transferred from one location to another.** | | | |
| **Requirements** | | **Description** | **Applies to** |
| T1 | Email and fax security statement | If using email or fax for communication or to collect data from subjects, include a statement to the subjects that email is not secure. | L2 – L5 |
| T2 | Email risk | If email or fax will be used to transmit research data, subjects should be cautioned to respond only from email addresses to which only they have access. | L3 – L5 |
| T3 | Fax security | Data are not faxed to a public fax machine. | L3 – L5 |
| T4 | Emailing or faxing PHI | Protected Health Information from UW Medicine should be transmitted by email only under the conditions described by UW Medicine policies. | L3 – L5 |
| T5 | Secure transmission | Electronic transmission of data over the internet, social media, or by text message must use cryptographic protocols, such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL) and a minimum key length of 28 bits. | L4 – L5 |
| T6 | Transportation of non-digital data | Transportation must occur via a method that ensures point-to-point tracking and delivery to only a verified, authorized individual. | L4 – L5 |
| T7 | Coordination of faxes | Arrangements are made so that the intended recipient will take the faxed material off of the machine immediately upon receipt. | L4, L5 |
| T8 | Transportation of highly sensitive data non-digital data | Transportation must occur via a method that is under the control of the study team (or designee) at all times. | L4 – L5 |

|  |  |  |  |
| --- | --- | --- | --- |
| **VENDORS: Non-University businesses or individual vendors who are hired on a contractual basis to perform specific research-related duties. Examples: a call center that administers surveys over the phone; a radiology service that is hired to read CT scans** | | | |
| **Requirements** | | **Description** | **Applies to** |
| V1 | Vendor contracts | The contract with the outside vendor providing research-related services must include requirements about how the confidentiality and security of the data will be maintained, including requirements related to:   * Users * Use of portable devices * Servers * Paper records and other non-digital storage media * Data transmission | L3 – L5 |