Committee for Protection of Human Subjects Data Security Requirements

The Committee for the Protection of Human Subjects (CPHS) has developed more robust and specific data requirements to more adequately protect the identifiable data used in research projects that require CPHS approval. These requirements apply to all researchers, their contractors and subcontractors with access to *Personally Identifiable Data (PID), which is defined as any data containing one or more of the Health Insurance Portability and Accountability Act (HIPAA) identifiers. Refer to 45 Code of Federal Regulations (CFR), Section 164.514(b)(2) or to the Glossary of Terms below for a listing of those identifiers. "Personal information" is also defined in the California Information Practices Act (IPA), Civil Code, Section 1798.3, as any information that identifies or describes an individual (see more specific data elements in the Glossary of Terms below).

If the researcher demonstrates that he or she is unable to comply with any of the requirements below, the researcher may request an exception from these requirements. An exception will only be granted if the researcher can demonstrate that adequate alternative measures have been taken to minimize risks so as to justify the exception.

Administrative Safeguards

All persons with access to PID are trained on privacy and security, and sign a confidentiality agreement. All persons with access to PID are subject to a background check, or a thorough reference check.

Researcher has obtained and submitted a statement form a governmental agency indicating that the release of the desired data is legal and that the agency is willing to release the desired data to the researcher

Researcher has committed that data will not be reused or provided to any unauthorized person or entity (unauthorized means that the person or entity does not have a need to access the data for purposes of the research project approved by CPHS).

Researcher has committed that information will not be published that could possibly be used to identify an individual subject.

Researcher has provided adequate justifications for the quantity of the data requested, the years and the variables.

Researcher has requested no more than the minimum necessary data to perform the research.

Access to data is limited only to those with a need to know for purposes of implementing or evaluating the research.

Researcher has justified why unique identifiers other than social security numbers cannot be used.

Researcher has committed to ensuring that subjects will not be identifiable in any published articles.

Researcher has described appropriate and sufficient methods to protect the identity of individual subjects when small cells or small numbers and/or data linkage to another data set are involved in the research project.

If the data set is to be linked with any other data sets, the Researcher has identified all data sets and each of the variables to be linked, with justification for each linkage.

If a third party is being used to perform data matching, Researcher has provided evidence of the third parties' ability to protect PID, including third parties' ability to comply with all the CPHS data security requirements.

Researcher will provide CPHS with a letter certifying that PID has been destroyed and/or return the disc with PID to the data source once research is concluded.

Chief Information Officer, Privacy Officer, or Security Officer or equivalent position of the researcher's institution will certify the CPHS Data Security Requirements are met.

Physical Safeguards

Research records will be protected through the use of locked cabinets and locked rooms; PID in paper form will not be left unattended unless locked in a file cabinet, file room, desk, or office.

Data will be destroyed or returned as soon as it is no longer needed for the research project.

PID in paper form is disposed of through confidential means, such as cross cut shredding or pulverizing.

Faxes with PID are not left unattended, and fax machines are in secure areas.

Mailings of PID are sealed and secured from inappropriate viewing; mailings of 500 or more individually identifiable records of PID in a single package, and all mailings of PID to vendors/contractors/co-researchers are sent using a tracked mailing method, which

includes verification of delivery and receipt, such as UPS, U.S. Express Mail, or Federal Express, or by bonded courier.

PID in paper or electronic form, e.g., stored on laptop computers and portable electronic storage media (e.g., USB drives and CDs), will never be left unattended in cars or other unsecured locations.

Facilities which store PID in paper or electronic form have controlled access procedures, and 24 hour guard or monitored alarm service.

All servers containing unencrypted PID are housed in a secure room with controlled access procedures.

Identifiers will be stored separately from analysis data.

All disks with PID will be destroyed

Electronic Safeguards

Computer access will be protected through the use of encryption, passwords, and other protections, as follows:

All workstations that contain PID have full disc encryption that uses FIPS 140-2 compliant software.

All laptops that contain PID have full disc encryption that uses FIPS 140-2 compliant software.

All PID on removable media devices (e.g. USB thumb drives, CD/DVD, smartphones, backup tapes) are encrypted with software which is FIPS 140-2 compliant.

All workstations, laptops and other systems that process and/or store PID have security patches applied in a reasonable time frame.

Sufficiently strong password controls are in place to protect PID stored on workstations, laptops, servers, and removable media.

Sufficient system security controls are in place for automatic screen timeout, automated audit trails, intrusion detection, anti-virus, and periodic system security/log reviews.

All transmissions of electronic PID outside the secure internal network (e.g., emails, website access, and file transfer) are encrypted using software which is compliant with FIPS 140-2.

PID in electronic form will not be accessible to the internet.

When disposing of electronic PID, sufficiently secure wiping, degaussing, or physical destruction is used.

Glossary of Terms

Personal Information is defined in the Information Practices Act (CC 1798.24(t) as, but is not limited to, name, social security number, physical description, home address, home telephone number, financial matters, and medical or employment history. It also includes statements made by, or attributed to, the individual.

Personally Identifiable Data (PID) is defined as the 18 HIPAA identifiers, listed below under "Identifiers".

Protected Health Information (PHI): Information in any format that identifies the individual, including demographic information collected from an individual that can reasonably be used to identify the individual. Additionally, PHI is information created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual.

De-identified: Information that has certain identifiers (see "identifiers" below) removed in accordance with 45 CFR 164.514; no longer considered to be Protected Health Information.

Identifiers: Under the HIPAA Privacy Rule "identifiers" include the following:

1. Names
2. Geographic subdivisions smaller than a state (except the first three digits of a zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000).
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death and all ages over 89 and all elements of dates (including year) indicative of such age (except that such ages and elements may be aggregated into a single category of age 90 or older)
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers

13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (excluding a random identifier code for the subject that is not related to or derived from any existing identifier).