

Summary of Changes to the DSHS Data Security Requirements Exhibit

In June of 2014, the Washington Department of Social and Health Services (DSHS) Human Research Review Section revised its Data Security Requirements Exhibit (DSRE) of the Confidentiality Agreement, which agreements are applicable to certain research in accordance with the Revised Code of Washington, Chapter 42.48.020(2). These revisions were made in order to conform with changes to the DSHS "Exhibit A - Data Security Requirements," and in response to the Department of Health and Human Services (DHHS) final rule issued on January 25, 2013 (78 FR 5565), which modified the HIPAA's Privacy, Security, and Enforcement Rules (45 CFR Part 160 and Subparts A and E of Part 164) to implement statutory amendments enacted pursuant to the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). The HITECH Act strengthens privacy and security protections for individuals' health information maintained in electronic health records and other formats. The DSRE was revised to incorporate the required regulatory provisions at 45 CFR 164, sections 164.504(e)(2)(C) and 504(e)(2)(D).

SUBSTANTIVE CHANGES:

- 1. Definitions** were added to clarify the meaning of terms, such as
 - Authorized RESEARCHER:** a RESEARCHER or RESEARCHERS with an authorized business requirement to access DSHS Confidential Information;
 - Hardened Password:** a string of at least 8 characters containing at least one alphabetic character, at least one number, and at least one special character, such as an asterisk, ampersand, or exclamation point; and
 - Unique User ID:** a string of characters that identifies a specific user, which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.
- 2. Specific instructions for transporting DSHS Confidential Data electronically** were added, including e-mail, specifying that the data will be protected by Transporting the Data within the (State Governmental Network) SGN or RESEARCHERS' internal network or encrypting any Data that will be in transit outside the SGN or RESEARCHERS' internal network. This includes transit over the public Internet.
- 3. Instructions for accessing data remotely** were modified to include the use of [Secure Access Washington \(SAW\)](#) which supersedes the requirement to encrypt data when it is accessed through this system.
- 4. Security for portable devices:** rules for portable devices have been modified to apply, "if those computers may be transported outside of a Secured Area."
- 5. Data Stored for backup purposes:** requirements for protecting backup media, and for destroying backup media, when it is retired while when DSHS Confidential Information still exists upon it, are outlined in the new Agreement.
- 6. Notification of Compromise or Potential Compromise:** in addition to the requirement to notify the Washington State Institutional Review Board (WSIRB) within one (1) business day of any

compromise of potential compromise of DSHS Confidential Data, the Agreement adds the obligation of RESEARCHERS to take actions to mitigate risk of loss and comply with any notification or other requirements imposed by law or DSHS.

7. **Subcontractors, sub-RESEARCHERS or Business Associates:** are now required to comply with all of the same data security requirements as the primary RESEARCHERS. Any contract between RESEARCHERS and subcontractors or sub-RESEARCHERS must include all of the data security provisions within the RESEARCHERS' Confidentiality Agreement, and within any amendments, attachments, or exhibits within that Agreement. If the RESEARCHERS cannot protect the Confidential Information as articulated within this Agreement, then the contract with the sub-RESEARCHERS must be submitted to the WSIRB for review and approval.

MINOR CHANGES:

In addition to the substantive changes articulated above, minor changes included: changing "data" to "DSHS Confidential Information" in most instances. "Contracted purpose" has been changed to "study purpose". "Other data" in the Data Segregation Section (Section 4) has been changed to "non-DSHS data". Completely defacing the readable surface with a coarse abrasive has been added to the acceptable methods of destroying Confidential Information on Optical Discs (e.g. CDs or DVDs).

As the DSRE revisions conform to applicable law, the DSRE revisions are not negotiable.