RESTRICTED DATA PROVIDER REQUIREMENTS CROSSWALK

Provider Name: Committee for Protection of Human Subjects (California Department of Public Health

Date Requirements retrieved: May 11, 2015
Source Requirements retrieved from:
http://www.oshpd.ca.gov/Boards/CPHS/DataSecurityRequirements.pdf

Physical Safeguards

#	Requirement	Met? (Yes/ No)	Notes
1	Research Records protected through 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	Yes	No PID will be produced in paper form. PID in electronic form on original media from provider will be stored in locked safe in secured area of NHDC
2	Data will be destroyed or returned as soon as it is no longer needed for the research project	Yes	Data will be destroyed at end of project term
3	PID in paper form is disposed of through confidential means, such as cross cut shredding or pulverizing	Yes	No printing is possible from SCRE
4	Faxes with PID are not left unattended, and fax machines in secure areas	Yes	No printing or faxing are allowed from SCRE
5	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	Yes	No printing is possible from SCRE
6	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	Yes	No printing is possible from SCRE
7	Facilities which store PID in paper or electronic form have controlled access procedures, and 24 hour guard or monitored alarm service	Yes	Electronic forms of PID are protected by NHDC access controls
8	All servers containing unencrypted PID are housed in a secure room with controlled access procedures	Yes	No unencrypted PID is permitted
9	Identifiers will be stored separately from analysis data	Yes	
10	All disks with PID will be destroyed	Yes	Research Guest VMs are wiped using Linux secure-delete (srm) command. Physical media containing PID will be destroyed at end of project.

RESTRICTED DATA PROVIDER REQUIREMENTS CROSSWALK

Electronic Safeguards

#	Requirement	Met? (Yes/No)	Notes
1	All work stations that contain PID have full disc encryption that uses FIPS 140-2 compliant software	Yes	All PID is stored on BitLocker (FIPS 140-2 mode) Encrypted disk image
2	All laptops that contain PID have full disc encryption that uses FIPS 140-2 compliant software	Yes	No laptops contain PID in the SCRE
3	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 complaint	Yes	No backups or copies of PID will be made to removable media from the SCRE
4	All workstations, laptops and other systems that process and/or store PID have security patches applied in a reasonable time frame	Yes	Updates and patches are checked for daily and applied daily on SCRE admin systems and Research VM Guest OSes
5	Sufficiently strong password controls and in place to protect PID stored on workstations, laptops, servers and removable media	Yes	14-character strong password consisting of uppercase, lowercase and numbers required for Windows login password, as well as Encrypted disk image Bitlocker password
6	Sufficiently strong security controls are in place for automatic screen timeout, automated audit trails, intrusion detection, anti-virus, and periodic system security/log reviews	Yes	Sufficient timeouts exist on the VPN portal, Windows sessions. Antivirus installed on all Windows systems and the File Transfer Gateway. System and application logs sent to a central logging host and reviewed regularly.
7	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.	Yes	No transmissions of electronic PID are permitted or possible outside of the secure internal network
8	PID in electronic form will not be accessible to the internet	Yes	No transmissions of electronic PID are permitted or possible outside of the secure internal network
9	When disposing of electronic PID, sufficiently secure wiping, degaussing or physical destruction is used.	Yes	Research Guest VMs are wiped using Linux secure-delete (srm) command. Physical media containing PID will be destroyed at end of project.