California Department of Public Health
California Neurodegenerative Disease Registry Data Use and Disclosure Agreement

This Data Use and Disclosure Agreement (Agreement) between the California Department of Public Health ("CDPH"), Chronic Disease Surveillance and Research Branch, Neurodegenerative Disease Registry ("CNDR") and _________________ [NAME OF DATA RECIPIENT] ("Recipient") sets forth the information privacy and security requirements Recipient is obligated to follow with respect to all personal and confidential information (as defined herein) Disclosed to Recipient by CNDR pursuant to this Agreement ("CNDR Data"). CDPH and Recipient desire to protect the privacy and provide for the security of CNDR Data Disclosed to Recipient, in compliance with state and federal laws applicable to CNDR Data.

I. Order of Precedence: With respect to information privacy and security requirements for all CNDR Data, the terms and conditions of this Agreement shall take precedence over any conflicting terms or conditions set forth in any other agreement between Recipient and CDPH.

II. Effect on Lower Tier Transactions: The terms of this Agreement shall apply to all contracts, subcontracts, and subawards, and the information privacy and security requirements Recipient is obligated to follow with respect to CNDR Data Disclosed to Recipient. When applicable, Recipient shall incorporate the relevant provisions of this Agreement into each subcontract or subaward to its agents, subcontractors, or independent consultants.

III. Definitions: For purposes of this Agreement, the following definitions shall apply:

A. Breach:

"Breach" means:

1. the unauthorized acquisition, access, Use, or Disclosure of Neurodegenerative Disease Registry in a manner which compromises the security, confidentiality, or integrity of the CNDR Data; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).

B. Confidential Information: "Confidential Information" means information that:

1. does not meet the definition of "public records" set forth in California Government code section 7920.530, or is exempt from Disclosure under any of the provisions of Section 7920.000, et seq. of the California Government code or any other applicable state or federal laws; or

2. is contained in documents, files, folders, books, or records that are clearly labeled, marked, or designated with the word “confidential” by CDPH.

C. CNDR Data: “CNDR Data” means Confidential Information collected and maintained by CNDR.

D. Disclosure: “Disclosure” means the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.

E. Personal Information: “Personal Information” means information, in any medium (paper, electronic, oral) that:

1. directly describes an individual; or

2. could be Used in combination with other information to indirectly identify or uniquely describe an individual, or link an individual to the information; or

3. meets the definition of “personal information” set forth in California Civil Code section 1798.3, subdivision (a); or

4. is one of the data elements set forth in California Civil Code section 1798.29, subdivision (g)(1) or (g)(2); or

5. meets the definition of “medical information” set forth in either California Civil Code section 1798.29, subdivision (h)(2) or California Civil Code section 56.05, subdivision (j); or

6. meets the definition of “health insurance information” set forth in California Civil Code section 1798.29, subdivision (h)(3); or

7. is protected from Disclosure under applicable state or federal law.

F. Security Incident: “Security Incident” means:

1. an attempted Breach; or

2. the attempted or successful unauthorized access or Disclosure, modification, or destruction of CNDR Data, in violation of any state or federal law or in a manner not permitted under this Agreement; or

3. the attempted or successful modification or destruction of, or interference with, Recipient’s system operations in an information technology system, that negatively impacts the confidentiality, availability, or integrity of CNDR Data; or

4. any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission; or

5. an information Security Incident may also include an event that constitutes a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies.

6. The term “Security Incident” shall not include pings and other broadcast attacks on Recipient’s firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in any defeat or circumvention of Recipient’s IT security infrastructure or in any unauthorized access to, or Use, or Disclosure of, CNDR Data.

G. Use: “Use” means the sharing, employment, application, utilization, examination, or analysis of information.

H. Workforce Member(s): “Workforce Member(s)” means an employee, contractor, agent, volunteer, trainee, or other person whose conduct, in the performance of work for Recipient, is under the direct control of Recipient, whether or not they are paid by Recipient.

IV. No HIPAA Business Associate Agreement or Relationship Between the Parties: This Agreement and the relationship it memorializes between the Parties does not constitute a business associate agreement or business associate relationship pursuant to Title 45, C.F.R., Part 160.103 (definition of “business associate”). The basis for this determination is Section 160.203(c) of Title 45 of the Code of Federal Regulations (see, also, [HITECH Act, § 13421, subdivision. (a)].). Accordingly, this Agreement is not intended to nor at any time shall result in or be interpreted or construed as to create a business associate relationship between the Parties.

V. Background and Purpose:

[For a Researcher:] Recipient desires to obtain CNDR Data for the purposes set forth in Recipient’s IRB approval.

[For all other recipients (the head of a state neurodegenerative disease registry/the head of a federal neurodegenerative disease control agency/local health officer):] Furthering the demographic, epidemiological, or other similar studies related to determining the sources of neurodegenerative diseases and evaluating measures designed to eliminate, alleviate, or ameliorate their effect.

VI. Use and Disclosure Restrictions: Recipient and its Workforce Member(s) shall protect CNDR Data from unauthorized Use or Disclosure. Recipient shall not Use or Disclose, except as otherwise specifically permitted by this Agreement, any CNDR Data to anyone other than CDPH personnel or programs without prior written authorization from the CDPH Program Contract Manager, except if Disclosure is required by State or Federal law. Recipient shall not Disclose or publish CNDR Data that may identify or reidentify a person in accordance with deidentification standards that are at least as stringent as the California Health and Human Services Data De-Identification Guidelines. In the event Recipient receives a subpoena or other compulsory legal process compelling disclosure of CNDR Data, Recipient shall notify CNDR within twenty-four (24) hours of receipt of the subpoena or other compulsory legal process and Recipient shall take legal steps to oppose the subpoena or other compulsory legal process at its sole expense.

VII. Legal Authority: The legal authority for CNDR to collect, create, access, Use, and Disclose CNDR Data to Recipient is Health and Safety Code sections 103871 and 103871.1 and Civil Code section 1798.24.

VIII. Means of Transmitting CNDR Data: CNDR data will be transmitted in a mutually agreed-upon format via Secure File Transfer Protocol (SFTP). Upon authorization and account setup, the approved recipient will be granted access to the data. Recipients must review all files for accuracy and completeness upon receipt. Any discrepancies or issues should be reported promptly to CNDRhelp@cdph.ca.gov.

IX. Safeguards: Recipient shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of CNDR Data, including electronic or computerized CNDR Data. At each location where CNDR Data exists under Recipient’s control, Recipient shall develop and maintain a written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of Recipient’s operations and the nature and scope of its activities in performing this Agreement, and which incorporates the requirements of Section X, Security, below. Recipient shall provide CDPH with Recipient’s current and updated policies within five (5) business days of a request by CDPH for the policies.

X. Security: Recipient shall take any and all steps reasonably necessary to ensure the continuous security of all computerized data systems containing CNDR Data. These steps shall include, at a minimum, complying with all of the data system security precautions listed in Recipient Data Security Standards set forth in Attachment 1 to this Agreement.

XI. Security Officer: At each place where CNDR Data is located, Recipient shall designate a Security Officer to oversee its compliance with this Agreement and to communicate with CDPH on matters concerning this Agreement.

XII. Training: Recipient shall provide training on its obligations under this Agreement, at its own expense, to all of its Workforce Member(s) who assist in the performance of Recipient’s obligations under this Agreement or otherwise Use or Disclose CNDR Data.

A. Recipient shall require Workforce Member(s) who receive training to certify, either in hard copy or electronic form, the date on which the training was completed.

B. Recipient shall retain Workforce Member(s) certifications for CDPH inspection for a period of three (3) years following contract termination or completion.

C. Recipient shall provide CDPH with its Workforce Member(s)' certifications within five (5) business days of a request by CDPH for the Workforce Member(s)' certifications.

XIII. Workforce Member(s) Discipline: Recipient shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other Recipient Workforce Member(s) under Recipient direct control who intentionally or negligently violate any provisions of this Agreement.

XIV. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: Recipient shall notify CDPH **immediately by telephone and email** upon the discovery of a Breach, and **within twenty-four (24) hours by email** of the discovery of any Security Incident, unless a law enforcement agency determines that the notification will impede a criminal investigation, in which case the notification required by this section shall be made to CDPH immediately after the law enforcement agency determines that such notification will not compromise the investigation. Notification shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XIV(F). If the Breach or Security Incident is discovered after business hours or on a weekend or holiday and involves CNDR Data in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH Information Security Office at the telephone numbers listed in Section XIV(F), below. For purposes of this Section, Breaches and Security Incidents shall be treated as discovered by Recipient as of the first day on which such Breach or Security Incident is known to Recipient, or, by exercising reasonable diligence would have been known to Recipient. Recipient shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a Workforce Member(s) or agent of Recipient.

Recipient shall take:

1. Prompt action to immediately investigate such Breach or Security Incident;

2. prompt corrective action to mitigate any risks or damages involved with the Breach or Security Incident and to protect the operating environment; and

3. any action pertaining to a Breach required by applicable state and federal laws, including, specifically, California Civil Code section 1798.29.

B. Investigation of Breach and Security Incidents: Recipient shall immediately investigate such Breach or Security Incident. As soon as the information is known and subject to the legitimate needs of law enforcement, Recipient shall inform the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer of:

1. what data elements were involved, and the extent of the data Disclosure or access involved in the Breach, including, specifically, the number of individuals whose Personal Information was Breached;

2. a description of the unauthorized persons known or reasonably believed to have improperly Used the CNDR Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the CNDR Data, or to whom it is known or reasonably believed to have had the CNDR Data improperly Disclosed to them;

3. a description of where the CNDR Data is believed to have been improperly Used or Disclosed;

4. a description of the probable and proximate causes of the Breach or Security Incident; and

5. whether Civil Code section 1798.29 or any other state or federal laws requiring individual notifications of Breaches have been triggered.

C. Written Report(s): Recipient shall provide written report(s) of the investigation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer as soon as practicable after the discovery of the Breach or Security Incident, and as further requested. The report(s) shall include, but not be limited to, the information specified above, as well as a complete, detailed corrective action plan, including information on measures that were taken to halt and/or contain the Breach or Security Incident, and measures to be taken to prevent the recurrence or further Disclosure of CNDR Data regarding such Breach or Security Incident.

D. Notification to Individuals: If notification to individuals whose information was Breached is required under state or federal law, and regardless of whether Recipient is considered only a custodian and/or non-owner of the CNDR Data, Recipient shall, at its sole expense, and at the sole election of CDPH, either:

1. make notification to the individuals affected by the Breach (including substitute notification), pursuant to the content and timeliness provisions of such applicable state or federal Breach notice laws. Recipient shall inform the CDPH Privacy Officer of the time, manner, and content of any such notifications, prior to the transmission of such notifications to the individuals; or

2. cooperate with and assist CDPH in its notification (including substitute notification) to the individuals affected by the Breach.

E. Submission of Sample Notification to Attorney General: If notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, and regardless of whether Recipient is considered only a custodian and/or non-owner of the CNDR Data, Recipient shall, at its sole expense, and at the sole election of CDPH, either:

1. electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content and timeliness provisions of Section 1798.29, subdivision (e). Recipient shall inform the CDPH Privacy Officer of the time, manner, and content of any such submissions, prior to the transmission of such submissions to the Attorney General; or

2. cooperate with and assist CDPH in its submission of a sample copy of the notification to the Attorney General.

F. CDPH Contact Information: To direct communications to CDPH staff, Recipient shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by verbal or written notice to Recipient. Said changes shall not require an amendment to this Agreement.

CDPH Program Contract Manager	**CDPH Privacy Officer**	**CDPH Chief Information Security Officer**
Catrina Taylor, PhD, MSPH Chief, Surveillance and Research Section Director, California Neurodegenerative Disease Registry California Department of Public Health Email:CNDRHelp@cdph.ca.gov Telephone: (916) 731-2500	Privacy Officer Privacy Office c/o Office of Legal Services California Department of Public Health P.O. Box 997377, MS 0506 Sacramento,CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413 Email: CDPH.InfoSecurityOffice@cdph.ca.gov Telephone: (855) 500-0016

XV. Documentation of Disclosures for Requests for Accounting: Recipient shall document and make available to CDPH or (at the direction of CDPH) to an individual such Disclosures of CNDR Data, and information related to such Disclosures, necessary to respond to a proper request by the subject individual for an accounting of disclosures of Personal Information as required by Civil Code section 1798.25, Confidential Information pursuant to Health and Safety Code section 103871, or any applicable state or federal law.

XVI. Requests for CNDR Data by Third Parties: Recipient and its Workforce Member(s), agents, or subcontractors shall promptly transmit to the CDPH Program Contract Manager all requests for Disclosure of any CNDR Data requested by third parties to this Agreement, unless prohibited from doing so by applicable state or federal law. The only instance in which this would not be required is if the person requesting the information or accounting of disclosures is the individual themselves, seeking information directly from Recipient as to all records directly held by Recipient.

XVII. Audits, Inspection and Enforcement: CNDR may inspect the facilities, systems, books, and records of Recipient as it may relate to CNDR, to monitor compliance with this Agreement. Recipient shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the CNDR Program Contract Manager in writing.

XVIII. Term: The term of this Agreement shall commence on the date below and remain in effect until [For Researchers: the expiration of the IRB Approval.] [For other Recipients: no longer than one year after this agreement is signed.] Any extended Use of CNDR Data shall be memorialized in an amendment to this Agreement or in a new agreement.

XIX. Termination:

A. Termination upon Breach: A Breach by Recipient of any provision of this Agreement, as determined by CNDR, shall constitute a material breach and grounds for immediate termination of this Agreement by CNDR. At its sole discretion, CNDR may give Recipient 30 days to cure the breach.

B. Judicial or Administrative Proceedings: Recipient will notify CNDR if it is named as a defendant in a criminal proceeding related to a violation of this Agreement. CNDR may immediately terminate the Agreement if Recipient is found guilty of a criminal violation related to this Agreement. CNDR may terminate this Agreement if a finding or stipulation Recipient has violated any security or privacy laws is made in any administrative or civil proceeding in which Recipient is a party or has been joined.

C. Termination without Cause: Either Party may terminate this Agreement without cause upon thirty (30) days written notice.

XX. Return or Destruction of CNDR Data Upon Request, Expiration or Termination: Upon (1) the request of CNDR due to mistaken disclosure by CNDR, or (2) the expiration or termination of this Agreement for any reason, Recipient shall securely return or destroy the CNDR Data. If return or destruction is not feasible, Recipient shall provide a written explanation to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XIV(F), above.

A. Retention Required by Law: If required by state or federal law, Recipient may retain, after expiration or termination, CNDR Data for the time specified as necessary to comply with the law.

B. Obligations Continue Until Return or Destruction: Recipient’s obligations under this Agreement shall continue until Recipient returns or destroys the CNDR Data or returns the CNDR Data to CNDR; provided however, that on expiration or termination of this Agreement, Recipient shall not further Use or Disclose the CNDR Data except as required by state or federal law.

C. Notification of Election to Destroy CNDR Data: If Recipient elects to destroy the CNDR Data, Recipient shall certify in writing, to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact information listed in Section XIV(F), above, that the CNDR Data has been securely destroyed. The notice shall include the date and type of destruction method used.

XXI. Amendment: The parties acknowledge that state and federal laws regarding information security and privacy rapidly evolve, and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such laws. The parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of CNDR Data. The parties agree to promptly enter negotiations concerning an amendment to this Agreement consistent with new standards and requirements imposed by applicable laws and regulations.

XXII. Assistance in Litigation or Administrative Proceedings: Recipient shall make itself and any subcontractors, Workforce Member(s), or agents assisting Recipient under this Agreement, available to CDPH at no cost to CDPH to testify as witnesses, in the event of litigation or administrative proceedings being commenced against CDPH, its director, officers, or employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by Recipient, except where Recipient or its subcontractor, Workforce Member(s) or agent is a named adverse party.

XXIII. No Third-Party Beneficiaries: Nothing express or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Recipient and their respective successors or assignees, any rights, remedies, obligations, or liabilities whatsoever.

XXIV. Interpretation: The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with state and federal laws and regulations.

XXV. Survival: If Recipient does not return or destroy the CNDR Data upon the completion or termination of the Agreement, the respective rights and obligations of Recipient under Sections IX, X and XIV of this Agreement shall survive the completion or termination of this Agreement.

XXVI. Choice of Law and Venue: The laws of the state of California will govern any dispute from or relating to this Agreement. The parties submit to the exclusive jurisdiction of the state of California and federal courts for or in Sacramento and agree that any legal action or proceeding relating to this Agreement may only be brought in those courts.

XXVII. Entire Agreement: This Agreement, including all attachments, constitutes the entire agreement between CNDR and Recipient. Any and all modifications of this Agreement must be in writing and signed by all parties. Any oral representations or agreements between the parties shall be of no force or effect.

[CONTINUES ON NEXT PAGE]

XXV. Signatures:

IN WITNESS, WHEREOF, the Parties have executed this Agreement as follows:

On behalf of Recipient, the undersigned individual hereby attests that they are authorized to enter into this Agreement and agrees to abide by and enforce all the terms specified herein.

____
(Name of Representative of Recipient)

____
(Title)

____
(Signature) (Date)

On behalf of CDPH, the undersigned individual hereby attests that they are authorized to enter into this Agreement and agrees to all the terms specified herein.

____
(Name of CDPH Representative)

____
(Title)

____
(Signature) (Date)

Attachment 1

Recipient Data Security Standards

I. Personnel Controls

A. ***Workforce Member(s) Training and Confidentiality.*** Before being allowed access to CNDR Data, all Recipient's Workforce Member(s) who will be granted access to CNDR Data must be trained in their security and privacy roles and responsibilities at Recipient's expense and must sign the confidentiality use statement attached hereto as Attachment 3 indicating they will not improperly Use or Disclose the CNDR Data to which they have access. Training must be on an annual basis. Acknowledgments of completed training and confidentiality statements, which have been signed and dated by Workforce Member(s) must be retained by Recipient for a period of three (3) years following contract termination. Recipient shall provide the acknowledgements within five (5) business days to CDPH if so requested.

B. ***Workforce Member(s) Discipline.*** Appropriate sanctions, including termination of employment where appropriate, must be applied against Workforce Member(s) who fail to comply with privacy policies and procedures, acceptable Use agreements, or any other provisions of these requirements.

C. ***Workforce Member(s) Assessment.*** Before being permitted access to CNDR Data, Recipient must assure there is no indication its Workforce Member(s) may present a risk to the security or integrity of CNDR Data. Recipient shall retain the Workforce Member(s)' assessment documentation for a period of three (3) years following contract termination.

II. Technical Security Controls

A. ***Encryption.***

- All desktop computers and mobile computing devices must be encrypted, in accordance with CDPH Cryptographic Standards or using the latest FIPS 140 validated cryptographic modules.

- All electronic files that contain CNDR Data must be encrypted when stored on any removable media type device (such as USB thumb drives, CD/DVD, tape backup, etc.), in accordance with CDPH Cryptographic Standards or using the latest FIPS 140 validated cryptographic modules.

- [data] must be encrypted during data in-transit and at-rest on all public telecommunications and network systems, and at all points not in the direct ownership and control of the Department, in accordance with CDPH Cryptographic Standards or using the latest FIPS 140 validated cryptographic modules.

B. ***Server Security.*** Servers containing unencrypted CNDR Data must have sufficient local and network perimeter administrative, physical, and technical controls in place to protect the CDPH information asset, based upon a current risk assessment/system security review.

C. ***Minimum Necessary.*** Only the minimum amount of CNDR Data required to complete an authorized task or workflow may be copied, downloaded, or exported to any individual device.

D. ***Antivirus software.*** Recipient shall employ automatically updated malicious code protection mechanisms (anti-malware programs or other physical or software-based solutions) at its network perimeter and at workstations, servers, or mobile computing devices to continuously monitor and take action against system or device attacks, anomalies, and suspicious or inappropriate activities.

E. ***Patch Management.*** All devices that process or store CNDR Data must have a documented patch management process. Vulnerability patching for Common Vulnerability Scoring System (CVSS) "Critical" severity ratings (CVSS 9.0 – 10.0) shall be completed within forty-eight (48) hours of publication or availability of vendor supplied patch; "High" severity rated (CVSS 7.0- 8.9) shall be completed within seven (7) calendar days of publication or availability of vendor supplied patch; all other vulnerability ratings (CVSS 0.1 – 6.9) shall be completed within thirty (30) days of publication or availability of vendor supplied patch, unless prior ISO and PO variance approval is granted.

F. ***User Identification and Access Control.*** All Recipient Workforce Member(s) must have a unique local and/or network user identification (ID) to access CNDR Data. To access systems/applications that store, process, or transmit CNDR Data, it must comply with SIMM 5360-C Multi-factor Authentication (MFA) Standard and NIST SP800-63B Digital Identity Guidelines. The SIMM 5350-C provides steps for determining the Authenticator Assurance Level (AAL), and a set of permitted authenticator types for each AAL (0-3). Note: MFA requirement does not apply to AAL 0.

All Recipient Workforce Member(s) are required to leverage Fast Identity Online (FIDO) authentication. The FIDO authentication is AAL 3 compliance. FIDO certified devices such as YubiKeys and Windows Hello for Business (WHfB) are the mechanism for user authentication in the Department.

Should a Workforce Member(s) no longer be authorized to access CNDR Data, or an ID has been compromised, that ID shall be promptly disabled or deleted. User ID's must integrate with user role-based access controls to ensure that individual access to CNDR Data is commensurate with job-related responsibilities.

	AAL 1	AAL 2	AAL 3
Permitted Authenticator Types	- Memorized Secret - Look-Up Secret - Out-of-Band Devices - Single-Factor One-Time Password (OTP) Device - Multi-Factor OTP Device - Single-Factor Cryptographic Software - Single-Factor Cryptographic Device - Multi-Factor Cryptographic Software - Multi-Factor Cryptographic Device	- Multi-Factor OTP Device - Multi-Factor Cryptographic Software - Multi-Factor Cryptographic Device - Memorized Secret **plus**: - Look-Up Secret - Out-of-Band Device - Single-Factor OTP Device - Single-Factor Cryptographic Software - Single-Factor Cryptographic Device	- Multi-Factor Cryptographic Device - Single-Factor Cryptographic Device used in conjunction with Memorized Secret - Multi-Factor OTP device (software or hardware) used in conjunction with a Single-Factor Cryptographic Device - Multi-Factor OTP device (hardware only) used in conjunction with a Single-Factor Cryptographic Software - Single-Factor OTP device (hardware only) used in conjunction with a Multi-Factor Cryptographic Software Authenticator - Single-Factor OTP device (hardware only) used in conjunction with a Single-Factor Cryptographic Software Authenticator and a Memorized Secret.

G. ***CNDR Data Destruction.*** When no longer required for business needs or legal retention periods, all electronic and physical media holding CNDR Data must be purged from Recipient's systems and facilities using the appropriate guidelines for each media type as described in the prevailing "National Institute of Standards and Technology – Special Publication 800-88" – "Media Sanitization Decision Matrix."

H. ***Reauthentication*.** Recipient's computing devices holding, or processing CNDR Data must comply the Reauthentication requirement, in which a session must be terminated (e.g., logged out) when the specified time is reached. Note: Reauthentication requirement does not apply to Authenticator Assurance Level (AAL) 0.

	AAL 1	AAL 2	AAL 3
Reauthentication	30 Days – Fix Period of Time, regardless user activity	12 hours – Fix Period of Time, regardless user activity; 30 minutes inactivity May use one of the authenticators to reauthenticate	12 hours – Fix Period of Time regardless user activity; 15 minutes inactivity Must use both authenticators to reauthenticate

In addition, reauthentication of individuals is required in the following situations:

- When authenticators change
- When roles change
- When the execution of privileged function occurs (e.g., performing a critical transaction)

I. ***Warning Banners.*** During a user log-on process, all systems providing access to CNDR Data, must display a warning banner stating that the CNDR Data is confidential, system and user activities are logged, and system and CNDR Data

Use is for authorized business purposes only. User must be directed to log-off the system if they do not agree with these conditions.

J. ***System Logging.*** Recipient shall ensure its information systems and devices that hold or process CNDR Data are capable of being audited and the events necessary to reconstruct transactions and support after-the-fact investigations are maintained. This includes the auditing necessary to cover related events, such as the various steps in distributed, transaction-based processes and actions in service-oriented architectures. Audit trail information with CNDR Data must be stored with read-only permissions and be archived for six (6) years after event occurrence. There must protect audit information and audit logging tools from unauthorized access, modification, and deletion. There must also be a documented and routine procedure in place to review system logs for unauthorized access.

K. ***Live Data Usage.*** Using live data (production data) for testing and training purposes is not allowed. Synthetic data must be Used. If synthetic data cannot be generated and/or Used, a de-identification process against the live data must be done to reduce privacy risks to individuals. The de-identification process removes identifying information from a dataset so that individual data cannot be linked with specific individuals. Refer to California Health and Human Services Data De-Identification Guidelines.

L. ***Privileged Access Management (PAM).*** Recipient is responsible for setting up and maintaining privileged accounts related to CDPH electronic information resources shall comply with the CDPH PAM Security Standard. Information resources include user workstations as well as servers, databases, applications, and systems managed on-premises and on the cloud.

M. ***Intrusion Detection***. All Recipient systems and devices holding, processing, or transporting [data] that interact with untrusted devices or systems via Recipient's intranet and/or the internet must be protected by a monitored comprehensive intrusion detection system and/or intrusion prevention system.

III. Audit Controls

A. ***System Security Review.*** Recipient, to assure that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection for CNDR Data, shall conduct at least, an annual administrative assessment of risk, including the likelihood and magnitude of harm from the unauthorized access, Use, Disclosure, disruption, modification, or destruction of an information system or device holding processing, or transporting CNDR Data, along with periodic technical security reviews using vulnerability scanning tools and other appropriate technical assessments.

B. ***Change Control.*** All Recipient systems and devices holding, processing, or transporting CNDR Data shall have a documented change control process for hardware, firmware, and software to protect the systems and assets against improper modification before, during, and after system implementation.

IV. Business Continuity / Disaster Recovery Controls

A. ***Emergency Mode Operation Plan.*** Recipient shall develop and maintain technical recovery and business continuity plans for systems holding, processing, or transporting CNDR Data to ensure the continuation of critical business processes and the confidentiality, integrity, and availability of CNDR Data following an interruption or disaster event lasting more than twenty-four (24) hours.

B. ***CNDR Data Backup Plan.*** Recipient shall have a documented, tested, accurate, and regularly scheduled full backup process for systems and devices holding CNDR Data.

V. Paper Document Controls

A. ***Supervision of CNDR Data.*** CNDR Data in any physical format shall not be left unattended at any time. When not under the direct observation of an authorized Recipient Workforce Member(s), the CNDR Data must be stored in a locked file cabinet, desk, or room. It also shall not be left unattended at any time in private vehicles or common carrier transportation, and it shall not be placed in checked baggage on common carrier transportation.

B. ***Escorting Visitors.*** Visitors who are not authorized to see CNDR Data must be escorted by authorized Workforce Member(s) when in areas where CNDR Data is present, and CNDR Data shall be kept out of sight of visitors.

C. ***Removal of CNDR Data.*** CNDR Data in any format must not be removed from the secure computing environment or secure physical storage of Recipient, except with express written permission of CDPH.

D. ***Faxing and Printing.*** Recipient shall control access to information system output devices, such as printers and facsimile devices, to prevent unauthorized individuals from obtaining any output containing CNDR Data. Fax numbers shall be verified with the intended recipient before transmittal.

E. ***Mailing.*** Mailings of CNDR Data shall be sealed and secured from damage or inappropriate viewing to the extent possible. Mailings which include five hundred (500) or more individually identifiable records of CNDR Data in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of CDPH to use another method is obtained.

Attachment 2
Recipient Breach and Security Incident Contact Information.

The following Recipient contact information must be included in the executed Agreement.

Recipient Program Manager	**Recipient Privacy Officer**	**Recipient Chief Information Security Officer (and IT Service Desk)**
Name	Name	Name
Title	Title	Title
Address	Address	Address
Address 2	Address 2	Address 2
City	City	City
State, Zip Code	State, Zip Code	State, Zip Code
Telephone	Telephone	Telephone
Email	Email	Email

Attachment 3

Confidentiality Use Statement

By signing this Confidentiality Use Statement, I agree to the following:

1. I have read the *Data Use Agreement* (“DUA”) between the California Neurodegenerative Disease Registry (“CNDR”) and the person or entity identified as the Recipient in said Agreement and agree to be bound by the terms in it.

2. I will safeguard the confidentiality of all confidential information contained in data provided by CNDR (“CNDR Data”) to which I will be given access in accordance with the terms of the DUA, and I will not in any way divulge, copy, release, sell, loan, review, or alter any CNDR Data except as within the scope of my duties.

3. I will only access CNDR Data for which I have a need to know, and I will use that information only as needed to perform my duties.

4. I will promptly report activities by any individual or entity that I suspect may compromise the availability, integrity, security, or privacy of CNDR Data to the Recipient and/or CNDR.

5. I understand that ownership of CNDR Data is vested solely in CNDR.

6. I understand that violating applicable laws and regulations governing the use and disclosure of CNDR Data may result in civil and criminal penalties.

Signature: ___________________________________ Date: _________________

Print Name: _________________________________

Please retain a copy for your records.