Electronic Data Sharing Agreement

Requester

Agency Name:	Lake County
County Representative:	Stephen Carter Jr.
Title:	Interim Behavioral Health Director and Assistant County Office Administrator
Address:	6302 Thirteenth Avenue, Lucerne CA 95458
Phone:	707-274-9101

I. PURPOSE

This Electronic Data Sharing Agreement (EDSA) is intended to facilitate a health care information exchange between California Correctional Health Care Services (CCHCS)/ California Department of Corrections and Rehabilitation (CDCR) and Lake County (County Agency) in compliance with all applicable federal, state, and local laws, regulations, and policies. This is intended to be the sole EDSA for the sharing of electronic health care information between both entities.

The Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires a Memorandum of Understanding between governmental entities with respect to the receipt, access, use, and disclosure of protected health information (PHI) as defined by Code of Federal Regulations, Title 45, section 160.103. This EDSA further sets forth the obligations of both entities that access, use, and disclose protected health care data sets.

For purposes of this EDSA, references to CCHCS refer to actions or responsibilities of CCHCS. References to CDCR refer to actions or responsibilities of CDCR.

This EDSA sets forth a common set of terms and conditions in support of a secure interoperable data exchange between CCHCS/CDCR and County Agencies. The entities have agreed to receive and/or provide an exchange of health care data sets via the technology solution hosted by CCHCS/CDCR to support continuity of care and positive patient outcomes.

The entities recognize that many patient-inmates qualify for and participate in multiple state and county programs. Leveraging advances in technology may break down information silos between entities and provide the following benefits:

- Assure the privacy and security of data
- Improve patient outcomes
- Increase reliability of data

- Reduce duplication of health care treatment and/or costs
- Improve integration of patient-inmates as they transition to and from community services
- Promote an efficient approach to the delivery of health care services
- Improve accessibility and management of health information
- Improve program effectiveness, performance, and accountability
- Promote pre-discharge planning to mitigate COVID-19 risk for patient-inmates transitioning to the community from parole or early release programs.

II. TERM OF EDSA

The term of the EDSA is three (3) years from the date of execution of the MOU to which this EDSA is attached as an exhibit.

III. JUSTIFICATION FOR ACCESS

A. California's Post-release Community Supervision Act of 2011 along with court ordered population reduction measures and Assembly Bill 109 (AB109) have changed the landscape of California's criminal justice system. These reforms changed the types of offenders eligible to serve their sentences in state prison and enhanced the State's system of post-release supervision. With these reforms, it has become necessary to change or enhance the method for sharing health information between CCHCS/CDCR and County agencies. This can be accomplished utilizing an electronic transfer of information for patient-inmates who transfer, parole, or are released to the community and as mandated by Penal Code Section 3003.

   The timely sharing of electronic health care information through a secure file transfer portal (SFTP) solution will support a standardized process to ensure continuity of care per Penal Code section 3003, and facilitate positive patient outcomes between CCHCS/CDCR and County agencies for medical, mental health, dental, and substance use disorder treatment (SUDT)/medication assisted treatment (MAT).

   Coordination of patient health care services and public health crisis mitigation due to infectious disease threats between CCHCS/CDCR and County agencies decreases community health care costs by reducing the need to treat more serious or neglected health care conditions.

B. State and Federal Requirements Citations/Authority:

   - 42 United States Code 1320 d-6
   - Code of Federal Regulations, Title 42, section 2.31
   - Code of Federal Regulations, Title 45 sections 164.502(b) – (b)(2)(iii); 164.508; 164.524(c)(3); 164.530(i)(1)
   - CA Civil Code, sections 56.10;56.15; 56.17; 56.37
   - CA Health and Safety Code, sections 11845.5(c)(4); 123115(b); 120980(g); 124980(j)
   - Government Code section 8658

IV. DESCRIPTION OF DATA

When available, a continuity of care packet shall be shared between CCHCS/CDCR and County agencies. The packet shall include information necessary for the coordination of patient's health care needs. The following are general examples of health care information to be shared:

HEALTH CARE DATA SETS		

Laboratory Studies:
• Blood Gasses
• Hematology
• Coagulation
• Chemistry
• Toxicology and Drug Monitoring
• Urinalysis
• Immunology and Serology
• Body Fluids and Other Sources
• Miscellaneous Send Out
• Blood Bank Results
• Bacteriology
• Mycobacteriology
• Mycology
• Parasitology
• Virology
• Pathology Reports
• Infectious disease status
• COVID-19 rapid test or PCR test results
 	
Radiology:
• Computed Tomography
• Diagnostic Radiology
• Interventional
• Magnetic Resonance Imaging
• Mammography
• Nuclear Medicine
• Ultrasound
	Orders:
	• Active Medications
	  • Inpatient
	  • Outpatient
	  • Prescription
	
	Clinical Documents:
	• History and Physical Reports
	• Office Clinic Notes
	• Discharge Documentation
	• Laboratory Documentation
	• Laboratory Reports
	• Progress Notes
	
	Dental:
	• Dental Treatment Plan
	• Dental Chart
	• Periodontal Chart
	• Clinical Notes
	• Active Dental Treatment Requests
	• Health History form (most recent)
	• Dental Radiographs (from MiPACS)
		Mental Health:
		• History and Physical Reports
		• Progress Notes
		• Mental Health Assessment
		• Discharge Summaries
		• Psychological Testing Reports
		• Suicide Risk and Self-Harm Evaluation
		• Utilization Management (Level of Care Assessment)
		• Mental Health Pre-Release Disposition Review
		• Mental Health Master Treatment Plan
		• Advanced Directive Documents
		• TB Reports
		• Medication Records

V. METHOD OF DATA ACCESS OR TRANSFER

To ensure the safe and timely transfer of health care data sets, both entities will utilize the CCHCS/CDCR SFTP solution. This solution is designed to be compliant with information security and HIPAA requirements. CCHCS/CDCR and the County Agency, including subcontractors, will establish specific safeguards to ensure the confidentiality and security of health care information and/or Personally Identifiable Information (PII)/Protected Health Information (PHI). PII/PHI shall be encrypted prior to the electronic transfer and transmissions will be consistent with the rules and standards promulgated by Federal statutory requirements regarding the electronic transmission of PII/PHI.

To ensure the safe and timely availability of pre-release data sets to counties for public health and early release parole purposes, the County Agency shall access data through two available data portals: the CDCR Release Tracking Tool – Public Health Version, and the CDCR Release Tracking Tool – Parole Version through a secure VPN portal.

VI. SFTP CUSTODIAL ROLES AND RESPONSIBILITY

For the duration of this EDSA, the entities mutually agree that CCHCS/CDCR will be designated as Custodian for the SFTP site and will be responsible for the maintenance and ongoing portal support. Both entities shall observe all conditions for the use and disclosure of health care data sets. CCHCS/CDCR will ensure the establishment of security agreements as specified in this EDSA to prevent unauthorized use. This EDSA represents and ensures; except as specified or except as authorized in writing, such health care data sets shall not be disclosed, released, revealed, showed, sold, rented, leased, or loaned to unauthorized entities. Access to the health care data sets covered by this EDSA shall be limited to the minimum number of individuals necessary to achieve the purpose stated in this section and to those individuals on a need-to-know basis only.

Note that, all PII/PHI remains within the purview of the treating health care entities. Health care data sets shall not be released to outside entities unless the release meets the conditions set forth in State and Federal HIPAA, Privacy rules and regulations; and compliance with Federal Regulations for SUDT/MAT Code of Federal Regulations, Title 42, Part 2.

Information Security: CCHCS/CDCR and the County Agency shall comply with the information security standards outlined below.

A. General Security Controls

   a. Confidentiality Statement: All persons authorized to access the SFTP site shall sign a confidentiality statement. The statement shall include at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement shall be signed by the workforce member prior to access to the SFTP site. CCHCS/CDCR will obtain renewals of this statement annually. CCHCS/CDCR shall retain each person's written confidentiality statement for inspection for a period of six years following contract termination.

b. Workforce Member Assessment: CCHCS/CDCR and the County Agency, to the extent consistent with their governing statutes, regulations, existing contracts, rules and policies, shall ensure that all workforce members that have access to the SFTP site have been assessed to ensure that there is no indication that the workforce member may present a risk to the security or integrity of data contained in the SFTP site. CCHCS/CDCR and the County Agency shall retain each workforce member's assessment documentation, whether in physical or electronic format, for a period of six years following contract termination.

c. Workstation/Laptop Encryption: All workstations and laptops that process and/or access the SFTP site must be encrypted using a FIPS 140:2 certified algorithm, such as Advanced Encryption Standard (AES), with a 256bit key or higher. The encryption solution must be full disk unless approved by the CCHCS/CDCR Information Security Office.

d. Server Security: Servers containing unencrypted health care data sets must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

e. Minimum Necessary: Only the minimum necessary amount of health care data sets required to ensure continuity of care and to perform necessary business functions may be accessed, viewed, copied, downloaded, or exported.

f. Removable Media Devices: All electronic files that contain health care data sets must be encrypted when stored on any removable media or portable device (i.e., USB thumb drives, floppies, CD/DVD, smart devices, tapes, etc.). Health care data sets must be encrypted using a FIPS 140:2 certified algorithm, such as AES, with a 256bit key or higher.

g. Antivirus Software: All workstations, laptops, and other systems that process and/or store health care data sets must install and actively use a comprehensive antivirus software solution with automatic updates scheduled at least daily.

h. Patch Management: All workstations, laptops, and other systems that process and/or store health care data sets must have operating system and security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

i. User IDs and Password Controls: All users shall be issued a unique user name for accessing the SFTP site. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the

password. Passwords are not to be shared and must be at least eight characters; must be a non-dictionary word; must not be stored in readable format on the computer; must be changed every 60 days; must be changed if revealed or compromised; and must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z);
- Lower case letters (a-z);
- Arabic numerals (0-9); and
- Non-alphanumeric characters (punctuation symbols).

j. Data Sanitization: All health care data sets must be sanitized using National Institute of Standards and Technology Special Publication 800:88 standard methods for data sanitization when the health care data sets are no longer needed.

B. System Security Controls

a. System Timeout: The system must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

b. Warning Banners: All systems containing health care data sets must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only. User must be forced to log off the system if they do not agree with these requirements.

c. System Logging: The system must maintain an automated audit trail which can identify the user or system process which initiates a request for health care data sets or which alters the health care data sets on the SFTP site. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If the health care data sets are stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least six years after occurrence.

d. Access Controls: The system must use role based access controls for all user authentications, enforcing the principle of least privilege.

e. Transmission Encryption: All data transmissions of the health care data sets outside the secure internal network must be encrypted using a FIPS 140:2 certified algorithm, such as AES, with a 256bit key or higher. This requirement pertains to any type of health care data sets in motion such as website access, file transfer, and email.

f. Intrusion Detection: All systems involved in accessing, holding, transporting, and protecting the health care data sets that are accessible via the SFTP site must be protected by a comprehensive intrusion detection and prevention solution.

C. Audit Controls

a. System Security Review: All systems processing and/or storing health care data sets must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.

b. Log Reviews: All systems processing and/or storing health care data sets must have a routine procedure in place to review system logs for unauthorized access.

c. Change Control: All systems processing and/or storing health care data sets must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of health care data sets.

D. Business Continuity/Disaster Recovery Controls

a. Disaster Recovery: CCHCS/CDCR and the County Agency must establish a documented plan to enable continuation of critical business processes and protection of the security of the SFTP site in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this EDSA for more than 24 hours.

b. Data Backup Plan: CCHCS/CDCR must have established documented procedures to backup the SFTP site to maintain retrievable exact copies of health care data sets. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore health care data sets should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CCHCS/CDCR data.

VII. PERMITTED USES AND REQUIREMENTS AFTER DATA TRANSFER

A. Paper Document Controls

a. Supervision of Data: The health care data sets in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk, or office. Unattended means that information is not being observed by an employee authorized to access the information. The health care data sets shall not be left unattended at any time in view of visitors or unauthorized individuals. In addition, health care data sets shall not be left unattended at any time in vehicles, planes, trains, or any other modes of transportation and shall not be checked in baggage on commercial airplanes.

b. Confidential Destruction: Health care data sets must be disposed of through confidential means, using NIST Special Publication 800:88 standard methods for data sanitization when the health care data sets are no longer needed.

c. Faxing: Faxes containing health care data sets shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.

d. Mailing: Health care data sets shall only be mailed using secure methods. Health care data set mailings shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted.

e. Email: Email containing sensitive, confidential, or personal information shall only be sent from a government-issued email address, shall only be sent to individuals who have a need to know, shall be encrypted before sending, and shall contain only the minimum necessary information required for the individual to perform the task from which the information is provided. The de-encryption code or password shall be sent to the recipient by separate email, and shall not be included in the email including the sensitive, confidential, or personal information.

VIII. CONFIDENTIALITY

CCHCS/CDCR and the County Agency each agree to maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the health care data sets and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established by the Federal Privacy Act and the California Medical Information Act (CMIA), Code of Federal Regulations, Title. 42, Part 2, and other state laws, regulations, and guidelines governing privacy and confidentiality will apply. (See Notice of Privacy Practices, Attachment 2)

Obligations of CCHCS/CDCR and the County Agency:

A. Uses and Disclosures of PII/PHI Data Sets

CHCHS/CDCR and the County Agency may use and disclose health care data sets only as permitted under the terms of this EDSA or as permitted by law, but shall not otherwise use or disclose the health care data sets and shall ensure that directors, officers, employees, contractors, and agents do not use or disclose the health care data sets in any manner that would constitute a violation of this EDSA.

B. Confidentiality

Each entity is independently responsible for abiding by the applicable laws and regulations pertaining to the health care data sets in their possession. Nothing in this EDSA shall relieve CCHCS/CDCR and the County Agency from abiding by relevant laws or regulations.

C. Minimum Necessary Information

CCHCS/CDCR and the County Agency agree that, to the extent that health care data sets are shared between CCHCS/CDCR and the County Agency, only the minimum necessary health care data sets shall be shared to ensure continuity of care.

D. Health Care Data Set Breaches

It is the responsibility of CCHCS/CDCR and the County Agency to comply with Privacy, HIPAA, the HITECH Act, the Omnibus Rule, Code of Federal Regulations, Title 42, Part 2, and applicable regulations, laws and statutes with respect to appropriate administrative, physical, and technical safeguards to protect PII/PHI. This pertains to any health care data sets shared between entities via the SFTP site. If any health care data sets are disclosed to an unauthorized entity, this is considered a health care information security event, otherwise known as a breach.

If CCHCS/CDCR and the County Agency enter into written agreements with any agents, subcontractors, vendors, business associates, or other provisioned users to whom entities in this EDSA provide PII/PHI received from or created or received by entities on behalf of CCHCS/CDCR and the County Agency, the entities agree to impose the same restrictions and conditions on such other entities above that apply to disclosure of health care data sets with respect to such PII/PHI under this EDSA. CCHCS/CDCR and the County Agency are directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of PII/PHI that are not authorized by this EDSA or required by law, including those uses and disclosures by the other entities above with whom the entities have contracted.

This EDSA includes the requirement that any security incidents or breaches of unsecured PII/PHI shall be reported to the covered entity or owner of the health care data sets. In accordance with Code of Federal Regulations, Title 45, section 164.504(e)(1)(ii), upon knowledge of a material breach or violation by the entity and/or its subcontractors, the respective entity shall report the information security incident and/or breach to:

CCHCS:ISO@cdcr.ca.gov
Or
(County's reporting address)

Each covered entity is responsible for their own breach reporting and shall notify the owner of the PII/PHI that a breach has occurred by completing the attached Information Security Incident Report packet. (See Attachment 1)

E. Breaches Committed by Subcontractors

It is the responsibility of each respective covered entity to cure the breach or end the violation and if necessary, terminate the EDSA if the subcontractor does not cure or end

the violation immediately as specified by Code of Federal Regulations, Title 45, section 164.408. However, if a subcontractor has breached a material term of the EDSA and cure is not possible, the CCHCS/CDCR and the County Agency shall terminate the subcontractor, unless there is mutual written agreement by CCHCS/CDCR and the County Agency.

IX. DISPOSITION OF DATA

CCHCS/CDCR shall delete all health care data sets from the SFTP site within 60 days. All electronic and paper copies containing PII/PHI shall be destroyed consistent with rules and regulations governing confidential records.

X. TRAINING

CCHCS/CDCR and the County Agency attest that each shall provide Information Security Awareness and Privacy Awareness training to all workforce members, contractors, business associates, or all other provisioned users with access to the SFTP site or who use the data shared through the site to comply with Privacy/HIPAA and information security best practices or as required by law.