Agreement Number: 20-00086
Memorandum of Understanding (MOU) Between the California Correctional Health Care Services and El Dorado County

Background

The California Correctional Health Care Services (CCHCS) Health Information Management (HIM) and El Dorado County (County Agency), pursuant to California Penal Code Section 3003(e)(2), are working collaboratively to facilitate the timely and efficient release of patient-inmate medical records between CCHCS HIM and County Agency for the purpose of ensuring continuity of care/coordination of care for medical, mental health, dental, and substance use disorder treatment. The two entities are working together to ensure secure transfer of Personally Identifiable Information (PII)/Protected Health Information (PHI).

Purpose

Effective upon execution for a duration not exceeding three (3) years, CCHCS and County Agency enter into this MOU for the purpose of secure transfer of PII/PHI, and/or HIPAA data between CCHCS and County Agency via CCHCS secure file transfer portal (SFTP). Transferred or downloaded information shall be in compliance with the Electronic Data Sharing Agreement (EDSA) (attached as Exhibit A) and all other applicable federal and state privacy and security related regulations and laws. County Agency agrees to safeguard all PHI downloaded from the CCHCS SFTP site pursuant to the terms of the EDSA.

This MOU addresses the conditions under which CCHCS and County Agency will release, exchange and use PII/PHI. This MOU shall serve as the sole agreement between the entities with respect to the use of PII/PHI and overrides any contrary instructions, directions, agreements, or other understandings in or pertaining to any other prior communication from CCHCS HIM or any of its components with respect to the information specified in this MOU.

The documents and information shared under this MOU will be used solely to provide continuity of care/coordination of care for health services as outlined and in response to California Penal Code Section 3003(e)(2), for patient-inmates transferred between CCHCS and County Agency.

County Agency agrees to the following:

1. County Agency shall contact CCHCS HIM to request and complete an enrollment packet.

2. County Agency shall notify HIM of any personnel or departmental changes that would affect the terms herein or information transferred while this MOU is in place.

3. County Agency agrees that only authorized users shall be provided access to the information to be transferred in this MOU. Any change of an authorized user shall be consistent with the instructions outlined in the County Health Care User Guide.

4. County Agency agrees to the prohibition of disclosing substance use disorder treatment and/or medication assisted treatment information to a third party not identified in this MOU without prior patient written consent unless required by law.

5. County Agency agrees to adhere to the specific privacy and security transmission safeguards required by CCHCS in the protocol of transfer of information outlined in the Specifications of Use (attached as Exhibit B).

6. Upon transfer of agreed patient-inmate information by CCHCS HIM, County Agency assumes its responsibilities for applicable laws related to protection and use of patient-inmate information pursuant to the terms in the EDSA (attached as Exhibit A).

7. The individual designated as the Information Custodian on behalf of the County Agency shall be responsible for the establishment and maintenance of privacy and security arrangements as specified in this MOU. Acknowledgement shall be made by execution of the SFTP County Secure Authorization Request (attached as Exhibit C) appointing an Information Custodian of the aforesaid file(s) by the County Agency and agreement to comply with the provisions of this MOU on behalf of County Agency.

8. Each entity shall ensure that all personnel who access the data covered by this MOU shall abide by all applicable information security and Privacy policies, including training, required by the respective entity as to its employees or contractors

9. The Information Custodian shall be required to sign a copy of the Security Awareness User Agreement (attached as Exhibit F) and Non-Redisclosure Agreement (attached as Exhibit G) and provide a copy to the HIM Point of Contact (POC) prior to the start of the MOU.

10. It is the responsibility of County Agency to provide CCHCS notice when a new Information Custodian is assigned. Any successor Information Custodian shall be required to sign a similar acknowledgement and provide to CCHCS a copy. Information Custodian shall maintain all original acknowledgment forms and certificates of training with the MOU file.

11. The Information Custodian shall ensure authorized users complete all requirements prior to being issued access.

12. County Agency agrees to abide by the EDSA (attached as Exhibit A)

CCHCS agrees to the following:

1. CCHCS System Administrators shall maintain access of any authorized user.

2. CCHCS agrees to adhere to the specific privacy and security transmission safeguards required by CCHCS in the protocol of transfer of information outlined in the Specifications of Use (attached as Exhibit B).

3. CCHCS agrees to abide by the EDSA (attached as Exhibit A)

Term

This Agreement shall be effective upon execution and expire three (3) years from date of execution, unless extended by CCHCS and County Agency before its expiration. This MOU shall be binding on any successors. The terms of this MOU and any amendments made to this MOU may only be modified in writing signed by both entities.

Termination

Either Party shall have the right to terminate the MOU by providing ninety (90) days written notice to the other Party at any time. If the MOU is terminated by either Party, steps shall be taken to ensure the termination does not affect any data-sharing already in progress.

On Behalf of County of El Dorado, the undersigned individual hereby attests that he/she has the authorization to bind its county to the terms of the MOU outlined and agrees to the terms and provisions specified herein:

Name	Title
Click here to enter text.	Click here to enter text.
Department	**Division**
Click here to enter text.	Click here to enter text.
Address	
Click here to enter text.	
Phone	**Email**
Click here to enter text.	Click here to enter text.
Signature	**Date**

On Behalf of California Correctional Health Care Services (CCHCS), the undersigned individual hereby attests that he/she has the authorization to enter into this MOU and bind the State to all of the terms and provisions specified herein:

Name	Title
Richard Robinson	Chief Privacy Officer
Department	**Division**
California Correctional Health Care Services	Privacy Office
Address	
8260 Longleaf Drive, Building C, Space C3-610, Elk Grove, Ca 95758	
Phone	**Email**
916-691-4424	Richard.Robinson@cdcr.ca.gov
Signature	**Date**

Electronic Data Sharing Agreement

Requester

Agency Name:	County of El Dorado Health and Human Services Agency
County Representative:	Nicole Ebrahimi-Nuyken, LMFT
Title:	Behavioral Health Director
Address:	768 Pleasant Valley Road, Diamond Springs, CA 95619
Phone:	530-621-6545

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 El Dorado 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 will breakdown 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

II. TERM OF EDSA

The term of the EDSA is three (3) years from the date of execution.

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 fundamentally changed the landscape of California's criminal justice system. These reforms drastically shifted 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 Senate Bill 76 (SB76), 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 AB109, satisfy the mandates of SB76, 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 between CCHCS/CDCR and County agencies decreases community health care costs by reducing the need to treat more serious or neglected health care conditions. Also, by providing timely, appropriate, and necessary health care services, there is a reduced risk of lawsuits and litigation costs.

B. State and Federal Requirements Citations:

   - 15 United States Code, section 45(a)
   - 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)

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
 	
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 exchange of health care data sets, both entities will utilize the CCHCS/CDCR SFTP solution. This solution is 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.

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, section 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. The statement shall be renewed annually. CCHCS/CDCR and the County Agency shall retain each person's written confidentiality statement for inspection for a period of six (6) 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 (6) 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 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 must 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 (6) 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.

E. 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.

VII. CONFIDENTIALITY

CCHCS/CDCR and the County Agency agree to establish 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, or business associates, 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.

VIII. 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.

IX. TRAINING

CCHCS/CDCR and the County Agency attest that each shall provide Information Security Awareness and Privacy Awareness training to all workforce members, contractors, and business associates 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.

CALIFORNIA CORRECTIONAL HEALTH CARE SERVICES

CCHCS
Information Security Incident Report
[revised 03/19]

Incident Number

Form Completion Instructions

Step 1: Upon discovering an incident, **immediately** contact your Manager and notify the Information Security Office (ISO) via e-mail at **CCHCS-ISO@cdcr.ca.gov**

Step 2: If this security incident involves protected health information related to a California Department of Public Health (CDPH) licensed facility you **MUST** complete this form and submit to CCHCS ISO **within 24 hours** of incident detection. For all other incidents at any facility or institution this form must be completed and submitted to CCHCS ISO within (3) three calendar days.

If you have any questions or need assistance in completing this report please contact the ISO using the contact information provided in step 1.

Step 3: This form must be complete (do not include any PHI or PII) and must include the following signatures :
A) Person Completing Report B) Manager C) Hiring Authority

Section 1: Incident Type *Check all that apply:*

☐ **State Data:** (includes electronic, paper, or any other medium)
- a) Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal. (See SIMM 5340-A).
- b) Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.
- c) Deliberate or accidental distribution or release of personal information by an agency, its employee(s), or its contractor(s) in a manner not in accordance with law or policy.
- d) Intentional non compliance by the custodian of information with his/her responsibilities.

☐ **Inappropriate Use or Unauthorized Access:** This includes actions of state employees and/or non-state individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems. This includes, but is not limited to, successful virus attacks, web site defacements, server compromises, and denial of service attacks.

☐ **Equipment:** Theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.

☐ **Computer Crime:** Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.

☐ Any other incidents that violate Agency policy.

Section 2: Contact Information

Name of Individual (s) involved:

Telephone Number: Division:

Email Address :

Incident Related To CDPH Licensed Facility? ☐ YES ☐ NO Incident Location Code: Select Site ASP

City, County and Zip Code:

Entity That Caused the Incident:

Manager's Name

Manager's Phone Number:

Todays Date:

Local IT Notified / Name:

Local IT Phone Number:

Section 3: Incident Details

Date Incident Occurred: Time Incident Occurred:

Date Incident Detected: Time Incident Detected:

Incident Location Address Line 1

Incident Location Address Line 2

City, State and Zip Code:

Has CDPH been notified?
(If related to a CDPH licensed facility) ◯ Yes ◯ No Date CDPH Notified:

Has law enforcement been contacted? (**Must report stolen equipment to law enforcement**) ◯ Yes ◯ No

Name of Law Enforcement Agency, Report #, POC

Section 3: Incident Details *-Cont'd-*

Incident Description:

Please include the following information in your detailed description:
The Location(s), The sequence of events, including estimated times and time frames, Means of discovery,
Full name(s) of individual(s), CDCR #(if inmate); affected by this incident, (do not include any PHI or PII) Describe if the incident's impact is internal/external (within CCHCS or an outside agency), Provide number of internal and/or external individuals affected, Any other relevant information.

Section 4: Details Of Data Involved

CCHCS data involved?	☐ Yes	☐ No	☐ N/A
Is the data classified as *Confidential* ?		☐ Yes	☐ No
Was the data encrypted ?		☐ Yes	☐ No

**If Yes, indicate what type of Confidential Information was involved? (check all that apply and/or include specifics Under Other)*

☐ Social Security Number(s)	☐ Financial	☐ Imaging	☐ Lab	☐ Dental
☐ Driver's License Number(s)	☐ Medical	☐ Mental Health	☐ Pharmacy	☐ Other*

*Other Please explain:

Section 4: Details Of Data Involved *-Cont'd-*

Describe the Data or Property Lost/Involved In The Incident:

(Please include specific details. Describe the following as applicable and relevant)
Data Involved (Describe Data) including names of persons affected e.g. inmate John Doe lab information was lost.
Equipment details including a) The Local Law Enforcement Agency, Officer, and Report Number b) Has service been terminated? c) Remote Wipe Initiated? d) Make/Model Number/Serial Number/Asset Tag Number any other relevant information.

Corrective Action Plan:

Please describe the action(s) that will be taken to recover the data and to protect the information from further disclosure if applicable. Was a recall initiated? Have you notified the unintended recipient(s)? What action(s) will be taken to prevent future occurrences. Also include the date(s) the actions were or will be implemented.)

Estimate the Cost of the Incident

(Please use $50.00 / hour and include the cost associated with the corrective action plan. Include replacement costs of the assets, information gathering, remediation activities, and time spent completing the report

Have Those Responsible For The Incident Been Identified ☐ Yes ☐ No

How Many Individuals Were Involved

Were State Employees Involved ☐ Yes ☐ No

Were other than State Employees Involved (does not include inmates) ☐ Yes ☐ No

If so, what is the name of their employer?

Section 5: Inmates

CDCR Inmates Involved? ☐ Yes ☐ No

Required if an inmate or parolee was involved:

Name of Supervising CDCR Employee

Inmate name and CDCR number? Attach Additional Pages as Needed

CDCR Policy and/or Procedure violated

☐ Other: Please explain:

Section 6: Signatures

Name of person completing this Form:

Signature: Date:

Name of the Immediate Manager of the Individual Involved:

Signature: Date:

Name of Hiring Authority

Signature: Date:

Section 7: Information Security Office USE ONLY

Information Security Officer's Full Name: Brian Colt

Signature: Date:

Cal CSIR Reportable Incident ☐ Yes ☐ No

Comments

Information Security Office
E-mail CCHCS-ISO@cdcr.ca.gov
Telephone 1-916-691-3243

Privacy Office
E-mail Privacy@cdcr.ca.gov
Telephone 1-877-974-4722

CCHCS Security Incident Reporting Procedures

1. According to SIMM 5340-A, a security incident is defined as follows:

a. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, procedures, or acceptable use policies.

i. **State Data** (includes electronic, paper, or any other medium).

1. Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal.
2. Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.
3. Deliberate or accidental distribution or release of personal information by a state entity, or its personnel in a manner not in accordance with law or policy.
4. Intentional non compliance by the custodian of information with his/her responsibilities.

ii. **Criminal Activity** Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.

1. **Unauthorized Access** This includes actions of state entity personnel and/or unauthorized individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems. Involving tampering, interference or damage to state data.
2. **Attacks** This includes, but is not limited to, successful virus attacks or exploited vulnerability, web site defacements, and denial of service attacks.

iii. **Equipment** This includes theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.

iv. **Inappropriate Use** This includes the circumventing of information security controls or misuse of a state information asset by state entity personnel and/or any unauthorized individuals for personal gain, or to engage in unauthorized peer-to-peer activity, obscene, harassing, fraudulent, illegal or other inappropriate activity

v. **Outages and Disruptions** This includes any outage or disruption to a state entity's mission critical systems or public-facing web applications lasting more than 2-hours, or in which the incident triggers the state entity's emergency response or technology recovery.

vi. **Any other incidents that violate state entity policy**.

2. If the incident meets the above criteria, the Program Unit must **immediately** take action and follow steps 3 – 5.

3. Complete the CCHCS Information Security Incident Form collecting the details and relevant information as required. "**CCHCS Information Security Incident Form,**"

4. The Program Unit or the person discovering the incident must immediately contact and report the incident to the CCHCS Information Security Office (ISO) using the following steps:

i. Email the ISO directly at CCHCS-ISO@cdcr.ca.gov or call **(916) 691-3243** with preliminary notice and summary of the events ***(e.g.: a description of the sequence of incident events, dates, location of the incident, people affected and full names, any lost data (personal or not,) any lost equipment and type of equipment … etc.)***

ii. **Supervisor or Hiring Authority Role:** In most cases, it is the supervisor or the hiring authority that must complete the Information Security Incident Report since the report involves collecting information on the incident that only supervisors or hiring authorities may be in a position to request from the employee who committed the incident.

iii. **The Local IT Role:** The Local IT is responsible for providing guidance and the technical substance to further enhance the completeness of the report.

iv. **Employee Relations Office:** If the incident involves possible employee disciplinary or internal investigation action, complete the Information Security Incident Report as accurately as possible, and contact the Employee Relations Officer (ERO) (916) 691-5857. The ERO will be responsible to contact the Office of Internal Affairs (OIA) and to coordinate the investigative activities

5. Within three **(3) business days** the Program Unit must complete the "**CCHCS Information Security Incident Form,**" and provide a **signed** copy of this form to the CCHCS ISO. **** Due to Regulatory and Legal obligations, the CCHCS Information Incident Form must be complete, must include ALL the requested information pertaining to the incident and be submitted within the timeframe outlined in this step.***

STATE OF CALIFORNIA
California Correctional Health Care Services

NOTICE OF PRIVACY PRACTICES

Effective: June 1, 2019

Your health information is personal and private. We are committed to protecting this information. We create a record of the care you receive. This record is needed to provide you with medically necessary care and to comply with certain legal requirements.

We are required by law to:

- Make sure that health care information that identifies you is kept private;
- Give you this notice of our legal duties and privacy practices with respect to your health care information;
- Follow the terms of the notice that is currently in effect; and
- Notify you of a breach of unsecured protected health information.

How We May Use and Disclose Your Health Care Information. The categories listed below describe the ways we use and disclose health care information. Not every possible use or disclosure is listed.

For Treatment. We may use your health care information to care for you. For example, we may disclose health care information about you to doctors in other health facilities who may be involved in your care.

For Payments, Refunds, and/or Reimbursements. We may share health care information to facilitate review of and payment for health care services provided to you. We solicit requests for reimbursement for services provided to you which are eligible for payments to us from federal programs, and may share health care information about you with other agencies which facilitate those reimbursements. We do this so we can coordinate payments for services and receive reimbursements or refunds. For example, we may give health care information to the Department of Health Care Services so we can receive eligible payments from federal funds for health care provided to you at outside hospitals.

For Health Care Operations. We may use and disclose health care information about you for health care operations. These uses and disclosures are necessary to deliver health care and make sure all of our patients receive quality care. For example, we may use health care information to review the treatment provided to you.

As Required by Law. We will disclose health care information about you when required to do so by federal, state, or local law. If we are required to report to the court concerning your condition, we may include health care information about you.

For Corrections Activities. We may disclose health care information about you when required for the maintenance, administration, safety, security, and good order of the correctional institution.

For Disclosure at Your Request. We may disclose health care information when requested by you. This will generally require your written authorization.

Workers' Compensation. We may release health care information about you for workers' compensation claims for work-related injuries or illness.

Public Health Risks. We may disclose health care information about you to public health agencies as permitted by law.

Health Oversight Activities. We may disclose your health care information to a health oversight agency for activities permitted by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose health care information about you in response to a court or administrative order. We may also disclose health care information about you in response to a subpoena, discovery request, or other legal proceeding by someone else involved in the dispute in accordance with federal and state privacy laws.

Inmates. As an inmate of a correctional institution or under the custody of a law enforcement official, we may disclose health care information in accordance with federal and state privacy law about you to the correctional institution or law enforcement official. These disclosures may be necessary for the institution to provide you with health care, to protect your health and safety or the health and safety of others, or for the safety and security of the correctional institution. We may also disclose health care information about you to a county health care facility or parole clinic to coordinate your follow-up care when leaving CDCR jurisdiction.

Statistical Analysis: We may use and disclose health care information about you for health care quality improvement projects, including statistical analysis. For example, a quality improvement project may involve comparing the health and recovery of all patients who received one medication to those who received another for the same condition. Statistical analysis projects may be subject to special approval and may also be subject to limits under federal or state law if considered "research."

Law Enforcement. In accordance with federal and state privacy laws, we may release a patient's health care information if asked to do so by a law enforcement official.

For Grievances Regarding This Notice. If you believe your privacy rights have been violated, you may file a health care grievance at your institution. All heath care grievances must be submitted in accordance with health care grievance regulations. **You will not be penalized in any way for filing a health care grievance**.

You may file a complaint with the Secretary of the federal Department of Health and Human Services. Submit any complaints to:

Centralized Case Management Operations
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F HHH Bldg.
Washington, D.C. 20201

SPECIFICATIONS OF USE

Information to be shared:

The minimum necessary health information shall be exchanged by both parties to ensure continuity of care. Department of Corrections and Rehabilitation (CDCR) to El Dorado County shall include information such as:

Medical Information:

- TB Chrono
- Health and Physical
- Health Information Summary

Substance-use Disorder Treatment Information:

- Substance Use Disorder records

Mental Health Information:

- Mental Health Evaluation (CDCR Form 7386)
- Mental Health Summary (CDCR Form 7387)
- Mental Health Treatment Plan (CDCR Form 7388)
- Brief Mental Health Evaluation (CDCR Form 7389)
- Abnormal Involuntary Movement Scale Examination for Tardive Dyskinesia (CDCR Form 7390)
- Suicide Risk Evaluation (CDCR Form 7447)

Dental Information:

- Dental information

The information contained in the data files to be provided to El Dorado County will be used by the county for identifying state Patient-inmates who are being released to the county for purposes of continuity of care/coordination of care and treatment as outlined in the aforementioned California Penal Code. This MOU is in effect for this purpose only.

SPECIFICATIONS OF USE

Information to be shared:

The minimum necessary health information shall be exchanged by both parties to ensure continuity of care. Department of Corrections and Rehabilitation (CDCR) to El Dorado County shall include information such as:

Medical Information:

- TB Chrono
- Health and Physical
- Health Information Summary

Substance-use Disorder Treatment Information:

- Substance Use Disorder records

Mental Health Information:

- Mental Health Evaluation (CDCR Form 7386)
- Mental Health Summary (CDCR Form 7387)
- Mental Health Treatment Plan (CDCR Form 7388)
- Brief Mental Health Evaluation (CDCR Form 7389)
- Abnormal Involuntary Movement Scale Examination for Tardive Dyskinesia (CDCR Form 7390)
- Suicide Risk Evaluation (CDCR Form 7447)

Dental Information:

- Dental information

The information contained in the data files to be provided to El Dorado County will be used by the county for identifying state Patient-inmates who are being released to the county for purposes of continuity of care/coordination of care and treatment as outlined in the aforementioned California Penal Code. This MOU is in effect for this purpose only.

CALIFORNIA CORRECTIONAL HEALTH CARE SERVICES

Exhibit C

Secure File Transfer Protocol Electronic Data Sharing Access Request Form

This form is used to add health care designees who are authorized to access health care records from California Correctional Health Care Services (CCHCS), Health Information Management (HIM) via Secure File Transfer Protocol (SFTP).

Authority:

Penal Code Section 3003(M)(2) requires the department to electronically transmit to the county agency responsible for community supervision the inmate's tuberculosis status, specific medical, mental health, outpatient clinic needs, and any medical concerns or disabilities for the purpose of identifying the medical and mental health needs of the individual.

Requester/User Information: **For County Clinical Patient Record Continuity of Care Access and Use Only**

REQUESTER/USER (PRINT NAME):		**COUNTY NAME**:
TITLE:		**COUNTY DEPARTMENT:**
E-MAIL ADDRESS: (FOR REQUESTER)		**COUNTY PROGRAM:**
TELEPHONE NUMBER:	**DATE OF REQUEST:**	**COUNTY ADDRESS:**

Training Certifications and Agreements:

Requester/User certifies the Training Certifications and Agreements have been successfully completed and acknowledges the training is required to be completed annually for each authorized user. Copies of the completed documents are attached to this request.

☐ Information Security Training	☐ Non Re-disclosure Agreement (NRDA)
☐ Privacy Training	☐ Security Awareness User Agreement (SAUA)

By signing this document you certify that you are aware of, understand, and are accountable for complying with CCHCS Information Security and Privacy Policies and will comply with all federal and state privacy laws regarding personally identifiable information ("PII") and protected health information ("PHI") entrusted to you as a user assigned and authorized by your county authorizer. Notice to the County Authorizer: When a health care designee is no longer authorized to access the SFTP site, a notification must be provided to County.SFTP.inquiries@cdcr.ca.gov.

COUNTY REQUESTER/USER (PRINT NAME):	**TITLE:**	**SIGNATURE:**	**DATE:**
***COUNTY AUTHORIZER (PRINT NAME):**	**TITLE:**	**SIGNATURE:**	**DATE:**

***County Authorizer is the person listed on the Memorandum of Understanding**

**********FOR CCHCS HIM STAFF USE ONLY**********

COMPLIANCE:

System Approver **by signing this form, you certify:**

It is appropriate to grant the requested access to the HIM_EDS SFTP folder.

AUTHORIZATION: SYSTEM OWNER SIGNATURE IS REQUIRED BEFORE ACCESS IS GRANTED

SYSTEM FOLDER OWNER (PRINT NAME):	TITLE:	SIGNATURE:	DATE:

Annual Information Security Awareness Training

Exhibit D

Chief Information Officer: Cheryl Larson

CALIFORNIA CORRECTIONAL
HEALTH CARE SERVICES

Introduction

Information security training is required by state and federal mandates. This course provides California Correctional Health Care Services (CCHCS) employees, contractors, and other personnel who have access to CCHCS information assets with the knowledge to protect the information system and sensitive data from internal and external threats.

D.A.N.G.E.R.

D: Define – What is Information Security

A: Acknowledge – Why is it important for YOU to protect information & investments

N: Notice – Recognize & notice a security threat when you see one

G: Guard – Take precautions to protect your information

E: Educate – Further Educate yourself about Information Security with these resources

R: Report – Report incidents

Define: What is Information Security?

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability of information.

Confidentiality

Protecting information from unauthorized disclosure to people or processes.

Integrity

Safeguarding the accuracy and completeness of information processing.

Availability

Ensuring that authorized users have access to information and associated assets when required.

Define: What is Information Security?

Privacy: A set of fair information practices to ensure that an individual's personal information is accurate, secure, and current, and that individuals know about the uses of their data.

Personally Identifiable Information (PII): Any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains.

Protected Health Information (PHI): Protected health information is defined as any information, in any form that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that can be used to identify an individual.

Health Insurance Portability and Accountability Act (HIPAA): Describes a list of specific direct identifiers that, along with a name, constitute individually identifiable information. If you have any one of these direct identifiers in your health information dataset, along with a name, you have PHI, and must be safeguarded appropriately.

Example: PHI could be a name with information regarding his/her Medi-Cal status.

Define: What is Information Security?

Direct Identifiers

- Name
- Address – street address, city, county, zip code, or other geographic codes
- Dates directly related to patient (except year), including DOB, admission or discharge date
- Telephone and/or FAX Numbers
- Driver's License Number
- E-mail Addresses
- Social Security Number
- Medical ID Number / CIN
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Any vehicle or device serial number, including license plates
- Web Addresses (URLs)
- Internet Protocol Address
- Photographic Images
- Any other unique identifying number, characteristic, or code

Acknowledge: Information Security is YOUR Responsibility

CCHCS employees are granted access to Internet and E-mail resources to provide education, research, marketing, procurement, and service opportunities in the performance of their duties.

Conduct all Internet and/or e-mail activities in a professional, lawful, and ethical manner. This includes the development of content of the Internet.

Accessing a personal or private Internet Service Provider for personal use while using any state equipment, or using non-state equipment for conducting state business, does not release an employee from the responsibility of complying with this policy.

Be aware that all employee computer activity is logged and monitored, all computer usage has an audit trail. Employees shall have no expectation of privacy for their use of department equipment.

CCHCS employees are granted access to information systems to perform their job functions on a need to know minimum necessary basis. If you feel you have access to “too much” information, speak to your supervisor.

Consequences

Organizational Consequences:

- Legal ramifications including civil and criminal for CCHCS
- Loss/misuse of sensitive information
- Injury or damage for those who have had their private information exposed
- Potential financial ramifications for those affected
- Reputation damage, loss of trust for CCHCS

Personal Consequences:

- Employee disciplinary action (written warning, suspension without pay, pay reduction, demotion, dismissal)
- Civil and criminal penalties (HIPAA violations)
- Fine up to $1.5 million and/or 10 years imprisonment
- Criminal prosecution for personal use – personal benefit

Notice: Recognize & notice a security threat or incident when you see one

A threat is a potential cause of an unwanted incident that may result in harm of an organization (agency) or a person.

Virus	Social Engineering
Worm	Shoulder Surfing
Trojan	Tailgating
BotNet	Phishing/Whaling
Adware	SQL Injections
Spyware	E-mail SPAM

Cyber Attack: Malicious attacks with the intent to cause major disruptions to our everyday government operations.

The Department of Defense (DoD) detects three million unauthorized “scans” or attempts by possible intruders to access official networks every day.

Notice: Recognize & notice a security threat or incident when you see one

A Security Incident may involve:

- Unauthorized disclosure, modification and or destruction of confidential information
- Inappropriate use or unauthorized access to computer systems
- Unintentional or inappropriate release of confidential information
- Theft, loss, damage or destruction of state equipment
- Use of a state computer to commit a crime

Examples include:

- Faxes or e-mails of PHI information to incorrect providers, organizations, beneficiaries, or individuals
- Mis-sent or lost documents including any form of protected information
- Mailings of PHI to incorrect providers, organizations, beneficiaries, or individuals
- Disclosures greater than minimum necessary to perform a job
- Password sharing
- Unauthorized viewing, access, or disclosure of confidential information
- Stolen laptop
- Lost mobile phone

Social Engineering: A common technique by hackers is to attempt to trick you by posing as an administrator or other person of authority to get CCHCS network and system information.

Phishing: Spear phishing scams will often appear to be from a department's own human resources or IT support and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can steal data.

*Per the State Administrative Manual (SAM)

Guard: Take precautions to protect your information

CCHCS uses administrative, physical and technical safeguards to protect PHI, PII, Confidential, and Sensitive Information.

Administrative Safeguards: Documented policies and procedures for day-to-day operations, managing the conduct of employees accessing the state's automated information systems and related devices, and managing the selection, development and use of security controls.

Examples: Policies, disaster recovery planning, risk management, training

Physical Safeguards: Security measures for protecting the Department's tangible information systems and confidential information, as well as related buildings and equipment from environmental hazards and unauthorized intrusion and theft.

Examples: Employee and visitor identification, locked desks and work spaces, shredding confidential information, caution when transmitting data, protecting mobile computing devices.

Technical Safeguards: Technology resources implemented to protect and improve the networking environment.

Examples: Encryption, Internet content filtering, anti-virus software, security patches, computer usage audit lodging, software install approvals, screen savers.

Guard: Take precautions to protect your information

Things TO DO to protect Information

Always lock your computer when unattended (CTRL+ALT+DELETE).	Conduct all Internet and / or e-mail activities in a professional, lawful, and ethical manner.
Store files on server / shared drives that are backed up; do not store on desktops.	Secure data in your possession from unauthorized access, including family members and friends.
Keep devices on you at all times, if you must leave a device unattended, store it in a protected, locked or inconspicuous space.	When left unattended, secure data in locked cabinets, locked drawers, locked rooms.
When feasible, cable lock your laptop to an immovable surface.	Lock up confidential destruct boxes when they are left unattended.
Return IT hardware including state computers, phones, hard drives, CDs, DVDs, flash drives etc. to your local IT for the proper sanitation and disposal.	Shred documents with confidential, sensitive or personal information, including protected health information.
Always ensure delivery to intended recipient by double checking e-mail address.	Minimize downloading or taking any CCHCS data outside the workplace.
Share the minimum necessary PHI / PII / ePHI / PCI / Confidential / Sensitive Information to get the job done.	Encrypt and password protect all mobile devices.
Use a password that is at least eight digits long and include at least three unique characters (upper case letters, lower case letters, numbers and / or non-alphanumeric characters.)	Consult with your supervisor or the Information Security Office if you have any questions. CPHCS-ISO@cdcr.ca.gov.

Guard: Take precautions to protect your information

Things NOT TO DO to protect Information

Do not use state owned computer equipment for any unauthorized purposes.	Do not download CCHCS data onto non-CCHCS authorized computers or mobile devices. This includes transferring data via thumb drives, CDs, etc.
When choosing a password, avoid common references and words from the dictionary e.g., our significant other's name, pet's name, birthday, favorite color, sequential (abc, 123, 555), easy to guess, etc.	Never send e-mail messages containing ePHI / PHI / PII / Confidential / sensitive information outside of the department unless you are authorized to do so and encrypt.
Never share your password(s) with anyone. Social engineers will try to trick you in an attempt to gain access to CCHCS information systems.	Do not e-mail CCHCS data to personal e-mail or other personally owned systems.
Do not use the same password for multiple systems.	Do not leave laptops in unattended vehicles or other locations where it may be easily taken.
Never open an unexpected – unrecognized e-mail attachment.	Do not leave PHI / PII / confidential information in public locations.
Do not release PHI, PII or ePHI without prior authorization and approval.	Do not install or download unauthorized software.

Guard: Take precautions to protect your information

Computer Equipment:

- Always lock your computer when unattended (CTRL+ALT+DELETE).
- Store files on server / shared drives that are backed up; do not store on desktops.
- Do not use computer equipment for any unauthorized purposes.

Mobile Devices:

- Keep devices on you at all times, if you must leave a device unattended, store it in a protected, locked or inconspicuous space.
- Mobile devices must be encrypted and password protected.
- When feasible, cable lock your laptop to an immovable surface.

Remote Access:

- Remote Access is a method to connect to the CCHCS network from remote locations in a very secure fashion. Always protect your computer by ensuring it has the latest security patches. Plug into the network at least every 30 days.
- Remote access has been known to be the most frequent method of exposure of PHI or ePHI leading to fines and personal liabilities.

Disposal of Information or Assets:

- Return IT hardware including state computers, phones, hard drives, CD's, DVD's, flash drives, etc. to your local IT for the proper sanitation and disposal.
- Printed documents must be shredded per government regulations.

HIPAA-Protected Information:

- Do not release PHI, PII or ePHI without prior authorization and approval.
- When approved for sharing PHI, PII, ePHI, share the minimum necessary.

Educate: Further Educate yourself about Information Security with these resources

It is important to know your organization's policies and procedures to ensure the highest level of information security.

For more information visit the following resources:

- CDCR Department Operations Manual (DOM)
- State Administrative Manual (SAM)
- The Information Practices Act
- Health Insurance Portability and Accountability Act – HIPAA – Security Rule
- Health Information Technology for Economic and Clinical Health (HITECH)
- Office of Health Information Integrity (Cal OHII)

Report: Report Incidents

If you feel there has been a threat or incident, immediately contact your manager and proceed with the following steps:

Report the incident to CCHCS Information Security Office (ISO) via E-mail CPHCS-ISO@cdcr.ca.gov and/or Telephone Number (916) 691-3242

Request and complete CCHCS Information Security Incident Form (ISIR) within (5) business days.

Information to collect:

- Date and time incident occurred, and detected
- Incident location
- General description of the incident
- How the incident was discovered
- The impact of the incident on the agency
- Type of information asset that was lost / breached (media, device, paper or electronic)
- Type of data breached / lost physical or electronic; protected / sensitive (SSN, medical record or CDC#, driver's license #, financial information, etc.)
- Corrective action plan (how this incident will be prevented in the future, and when you intend to correct the current incident.)
- Estimate cost of the incident

Submit the signed security incident form to the ISO.

HIPAA-Protected Information: If you suspect that a breach of PHI, ePHI, PII or other unauthorized release of information may have occurred immediately contact CCHCS Privacy Office at E-mail: privacy@cdcr.ca.gov or by phone Toll Free at 1-877-974-4772.

Prevent security breaches by remembering **D.A.N.G.E.R.**

D.A.N.G.E.R.

D: Define – What is Information Security

A: Acknowledge – Why is it important for YOU to protect information & investments

N: Notice – Recognize & notice a security threat when you see one

G: Guard – Take precautions to protect your information

E: Educate – Further Educate yourself about Information Security with these resources

R: Report – Report incidents

CCHCS Information Security Awareness Training Questions for External Entities

Please select one answer for each question

Question 1:

Information Security is the protection of information assets from:

a) Authorized users
b) Management
c) Untrained users
d) Hackers

Question 2:

Personally Identifiable Information (PII) contains the following identifiers:

a) Name, SSN, hometown
b) SSN, Name, DOB
c) Driver's license #, car color, year of birth
d) E-mail address, home address, eye color

Question 3:

When you see or encounter an incident, you should contact:

a) Your Chief Executive Officer (CEO)
b) Your Chief Information Officer (CIO)
c) The Information Security Officer (ISO)
d) 911

Question 4:

You should always use the same password for all your devices because it is easy to remember:

a) True
b) False

Question 5:

You should familiarize yourself with the CDCR Department Operations Manual (DOM) because it contains our CCHCS Information Security policy:

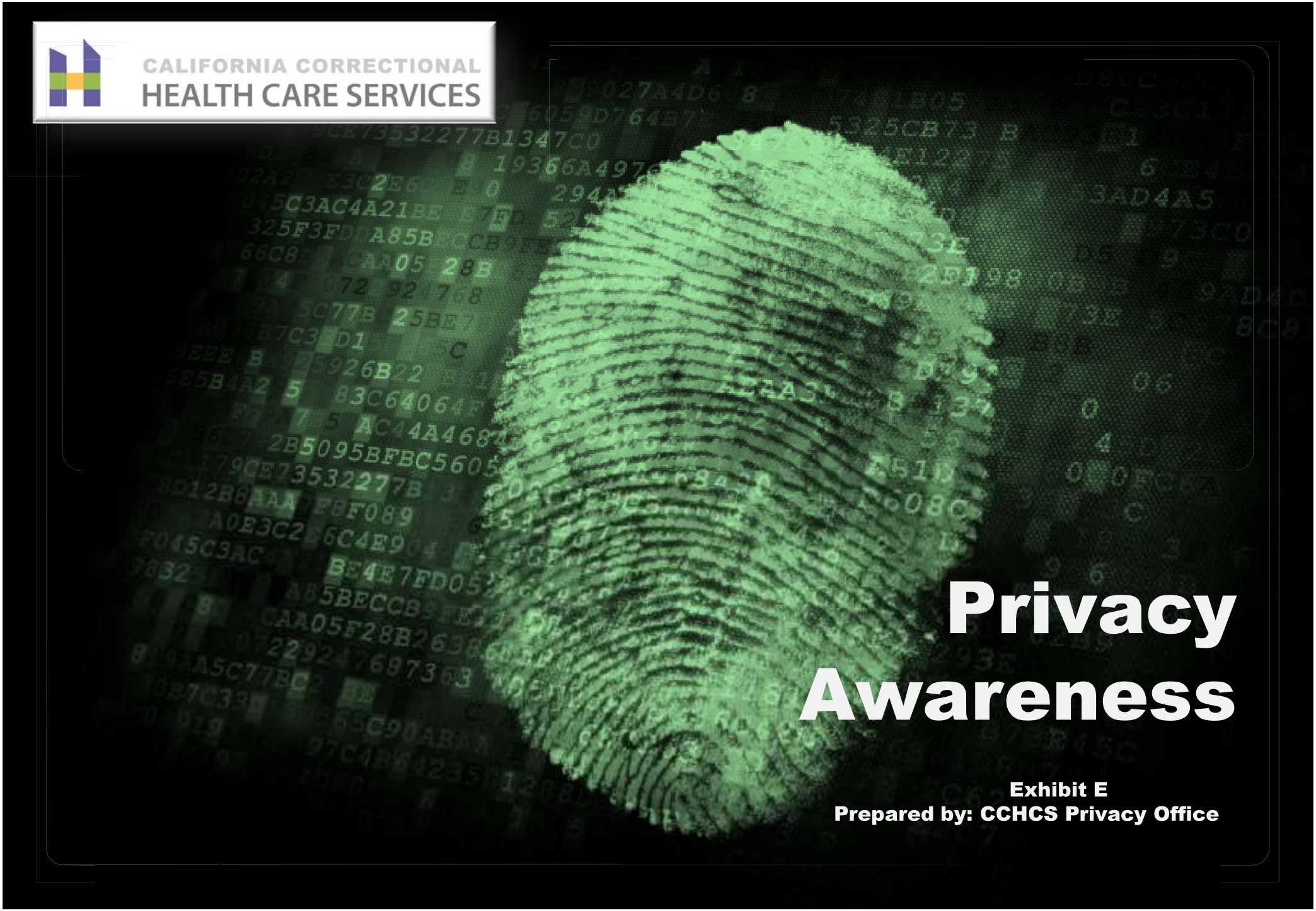
a) True
b) False

CALIFORNIA CORRECTIONAL
HEALTH CARE SERVICES

Information Security Awareness Training

I hereby attest that I have read and understand the information provided to me regarding Information Security

County	**Phone Number**
Name - Printed	**E-mail**
Signature	**Date**


CALIFORNIA CORRECTIONAL
HEALTH CARE SERVICES
Privacy Awareness
Exhibit E
Prepared by: CCHCS Privacy Office

Overview

This course provides an overview for:

- Privacy and understanding its importance
- Privacy laws, policies, and principles
- Your role in protecting privacy
- Consequences for violations
- How to report a privacy event

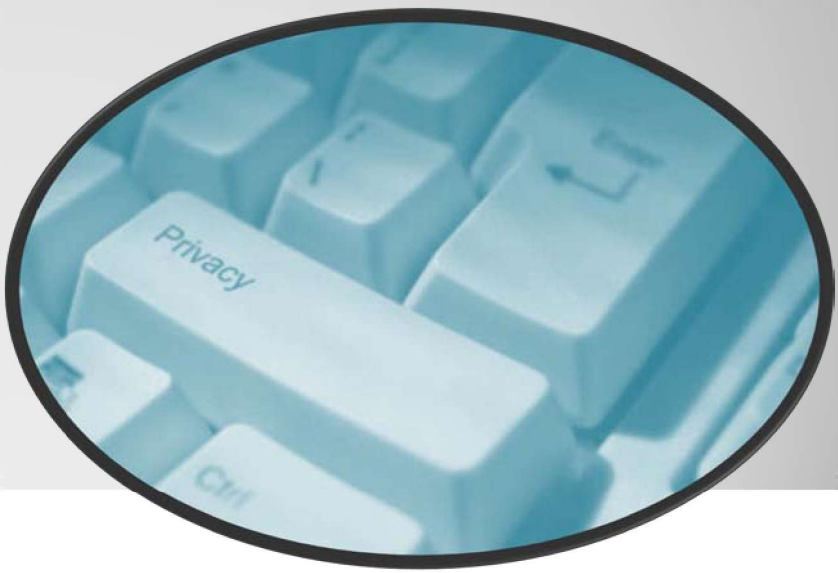
Learning Objectives

1. Recognize your role in protecting privacy.
2. Recognize the consequences for privacy violations.
3. Recognize how to report a privacy event.

What Is Privacy?

Privacy refers to freedom from intrusion into personal matters and personal information. It is a right rooted in common law.

At CCHCS privacy can relate to staff information, inmate information, electronic forms of information, hard copies, statements made verbally by individuals, etc.



Roles and Responsibilities

All members of the CCHCS workforce are responsible for following privacy policies and procedures, which include:

1. Create, collect, use, and disclose personal information for reasons that are for a legitimate job function, support the mission of CCHCS, and are allowed by law.
2. Disclose only the minimum amount of information necessary.
3. Access information only for authorized purposes.
4. Follow standards to safeguard personal information throughout the information life cycle.
5. Report suspected privacy violations or incidents.
6. Comply with all applicable privacy laws.

Possible Consequences of Privacy Violations

Privacy violations have several possible consequences:

- Embarrassment or harm to others
- Loss of trust between CCHCS and the public
- Employee discipline
- Personal fines
- Individual criminal charges

Key Privacy Laws

- Federal Privacy Act, Public Law 93-579
- Freedom of Information Act, 5 U.S.C. 552(b)(6)
- Information Practices Act, California Civil Code Section 1798 et seq.
- California Public Records Act, Government Code Section 6250 et seq.

Privacy Guidance and Policy

Guidance

Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining ***privacy as an inalienable right***.

The Information Practices Act of 1977 (Civil Code section 1798, et seq.) places ***specific requirements*** on ***each state entity*** in the collection, use, maintenance, and dissemination of information relating to individuals.

Government Code Section 11019.9 ***requires state agencies to*** "… maintain a privacy policy and to designate an employee to be responsible for the policy."

Government Code Section 11549.3 states that CCHCS shall **ensure *compliance*** with all privacy laws, regulations, rules, and standards specific to and governing the administration of their programs.

What is Personally Identifiable Information (PII/PHI)?

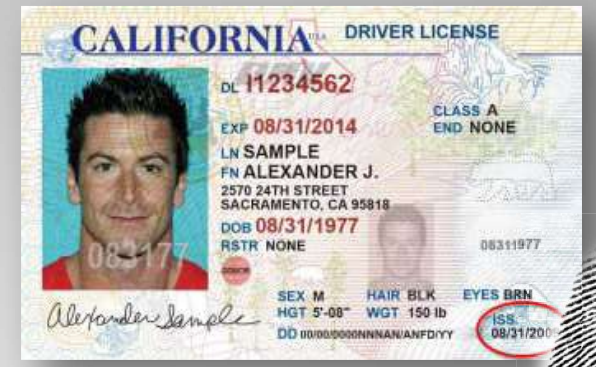
Per Civil Code 1798.3: Personal Information means any information that is maintained by an agency that identifies or describes an individual, **including, but not limited to**, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history.

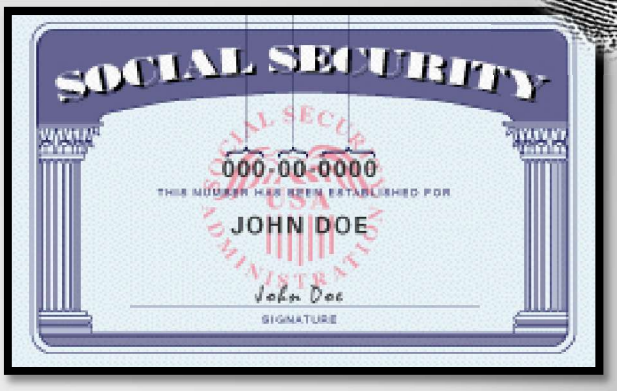
It also may include statements made by, or attributed to, the individual.

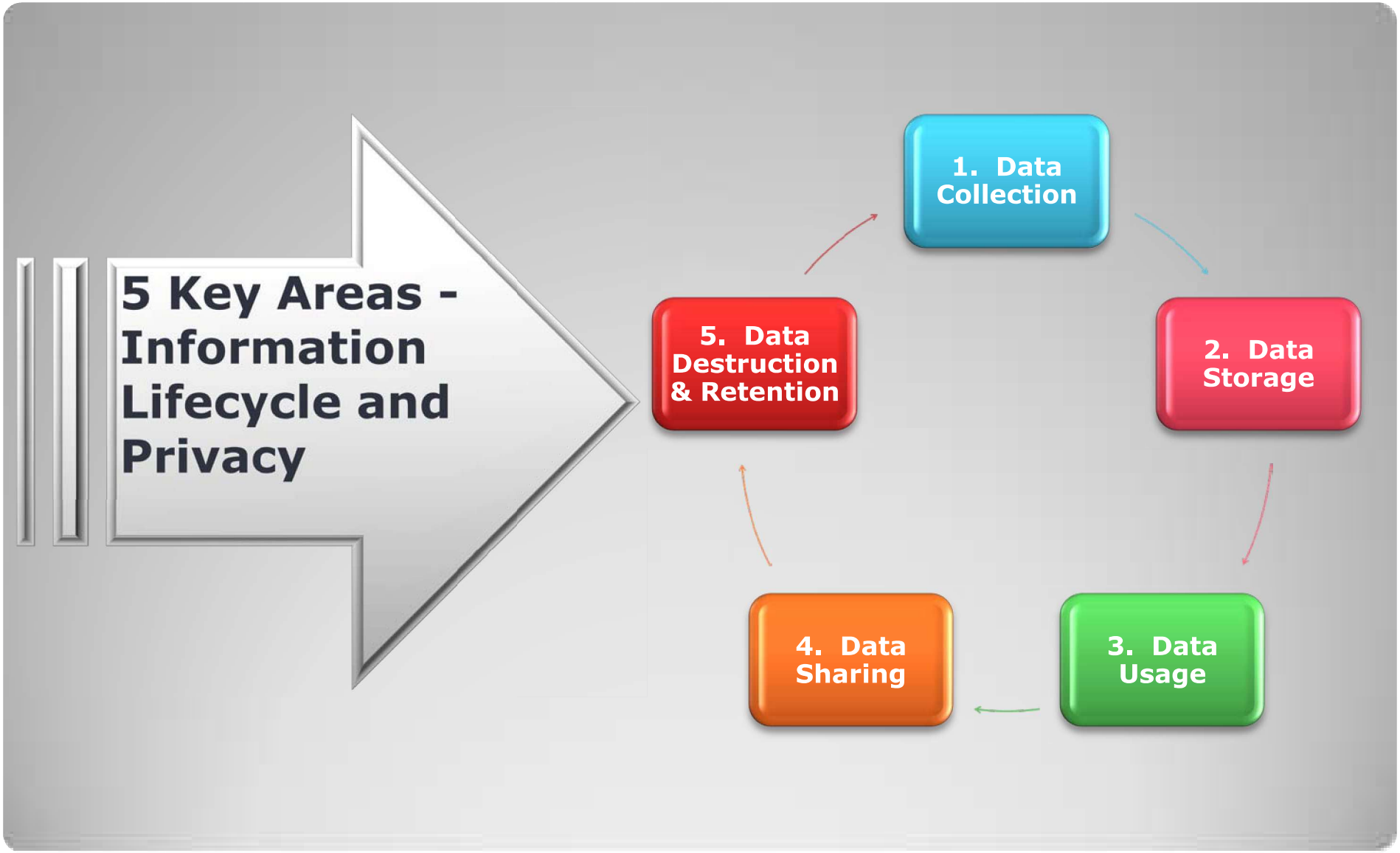
Common Examples of PII/PHI

(Typically a combination of two or more)

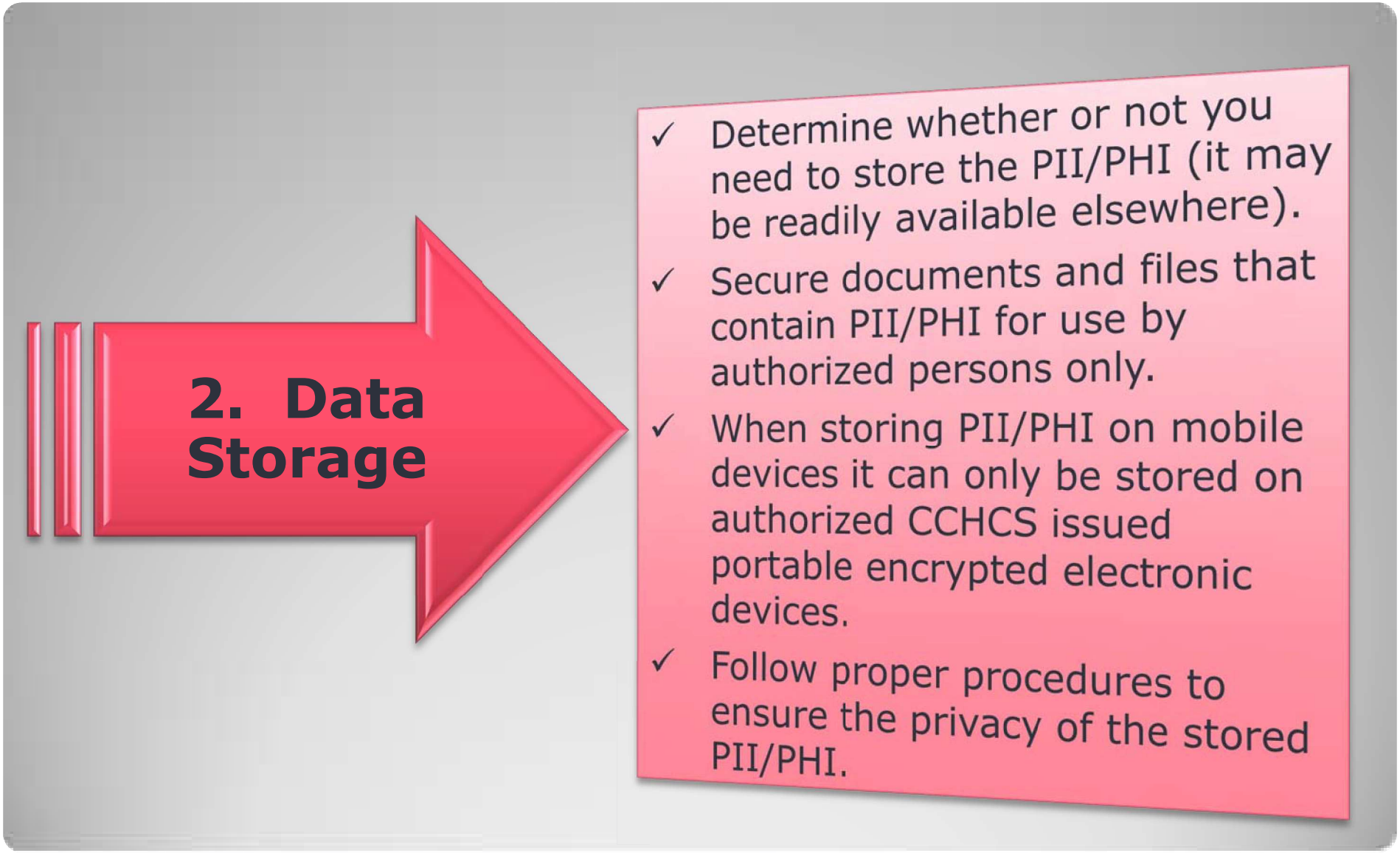
- Name
- Social Security number (SSN)
- Date of birth (DOB)
- Mother's maiden name
- Financial records
- Email address
- Driver's license number
- Passport number
- Health information
  - Including patient identification number

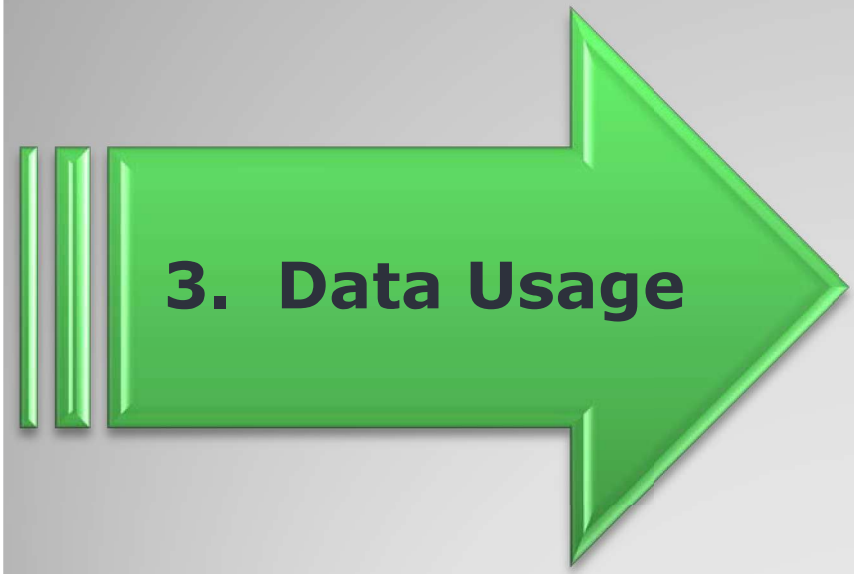





5 Key Areas - Information Lifecycle and Privacy
1. Data Collection
2. Data Storage
3. Data Usage
4. Data Sharing
5. Data Destruction & Retention

- ✓ Ensure you are allowed to collect the PII/PHI (law, regulation, policy, etc.).
- ✓ Validate you have a legitimate business need to collect the PII/PHI.
- ✓ Determine if you are obtaining the PII/PHI in a secure manner so it cannot be overheard or seen by others.
- ✓ Request, create, or collect only the minimum amount of PII/PHI necessary to do your job.


2. Data Storage
✓ Determine whether or not you need to store the PII/PHI (it may be readily available elsewhere).
✓ Secure documents and files that contain PII/PHI for use by authorized persons only.
✓ When storing PII/PHI on mobile devices it can only be stored on authorized CCHCS issued portable encrypted electronic devices.
✓ Follow proper procedures to ensure the privacy of the stored PII/PHI.



- ✓ Only use the PII/PHI for the purpose it was provided.
- ✓ Use only the minimum amount of PII/PHI necessary to complete your job functions.
- ✓ Access PII/PHI using authorized procedures.
- ✓ Use secure authorized equipment and technology connections.

- ✓ Verify the sharing is allowed.
- ✓ Validate that everyone sharing the PII/PHI has a need to know.
- ✓ Share only the minimum amount of PII/PHI and follow proper disclosure procedures.
- ✓ Make sure you share PII/PHI using the appropriate safeguards (e.g., encryption, sealed envelope).

- ✓ Ensure the PII/PHI has a valid retention schedule.
- ✓ Shred papers containing PII/PHI when no longer needed.
- ✓ Return unused equipment (e.g., computer, copiers, fax machines) to the IT department for proper disposal.

Differences Between Privacy and Information Security

The General Rule – "W" and "H"

Privacy: the "**W**" questions:

- **Why** am I creating, collecting, storing or sharing the PII/PHI?
- **What** are the data elements of the PII/PHI?
- **Who** am I collecting the PII/PHI from?
- **Who** am I going to share the PII/PHI with?
- **When** might I share the PII/PHI?
- **Where** am I going to store and save the PII/PHI?
- **When** am I going to need to destroy the PII/PHI?

Differences Between Privacy and Information Security

Information Security: the "**H**" questions:

- **How** am I going to securely create, collect, store and share PII/PHI to ensure it is private?
- **How** does CCCHS require me to ensure certain types of information are kept private?
- **How** do I find out the proper way to securely share information verbally, in writing and electronically to ensure privacy?
- **How** am I supposed to securely store and destroy PII/PHI?

What is a Breach of Privacy?

A privacy breach occurs when there is unauthorized access, collection, creation, use, or impermissible disclosure of private information.

Common Scenarios

Common privacy breaches include:

- Private conversations in public places.
- Paper and other documents stored in incorrect folders and accidently disclosed.
- Inadvertently sending email containing PII/PHI to a person not authorized to view it.
- Allowing an unauthorized person to use your computer.

The Effects of Compromised Privacy

Privacy breaches ARE SERIOUS; outcomes can include:

- Exploitation of an individual's medical/financial status
- Harm to unintended individuals
- Personal fines, sanctions, and fees
- Job loss
- Criminal charges and prison

How and When to Report

- ✓ Do not investigate an incident on your own.
- ✓ Immediately report suspected incidents within 3 days to the Information Security Office (ISO) via E-mail CCHCS-ISO@CDCR.ca.gov and/or Telephone Number (916) 691-3243.
- ✓ The ISO is the **first point** of contact for **all** information security incidents (even those that affect PII/PHI).
- ✓ Incidents relating to PHI and a California Department of Public Health (CDPH) licensed facility (e.g. General Acute Care Hospital) must be reported to the CCHCS ISO within **24 hours**. The facility must also follow their procedures for reporting to CDPH.

Policies and Procedures

- **It is your responsibility** to read, understand, and abide by CCHCS privacy policies and related policies and procedures.
- Policies can be found on the CCHCS Internet.
- You can request hard copies from your supervisor.

Privacy Guidance

For specific privacy-related policy questions:

- See Chapter 13 of the Inmate Medical Services Policy and Procedures Manual
- Email the CCHCS Privacy Office at privacy@cdcr.ca.gov
- Call the CCHCS Privacy Office 1-877-974-4722

Course Summary

This course provided you information on:

- The definition of privacy and understanding its importance.
- Privacy laws, policies, guidance, and principles.
- Your role in protecting privacy and the consequences for violations.
- Reporting a privacy breach.

How to Protect PII/PHI

For more information on how to protect PII/PHI, refer to the Information Security Awareness training.

Self-Certification of Completion

For County Business Associates

California Correctional Health Care Services Privacy Awareness Training

I certify I have completed the Privacy Awareness Training course. I have read, understand and shall comply with the California Correctional Health Care Services (CCHCS) Privacy policies, related policies and understand it is my responsibility to comply with related state and federal privacy law. I shall ensure a copy of this training certificate is maintained and can be provided upon request for at least six years.

Please complete all of the information below:

Name of County Facility/Jail:

_____

Unit Name (If applicable):

_____

Legibly PRINT Last Name:

_____

Legibly PRINT First Name:

_____

Phone:

_____

E-Mail:

_____

Manager's Name/Project Manager's Name (In MOU):

_____

Date Privacy Awareness Training completed:

_____

Contractors complete this section:

Name of County:

_____

MOU Agreement Number:

_____

_____ _____ _____ _____

Signature *Date* *EDSA Manager's Signature* *Date*

CALIFORNIA CORRECTIONAL HEALTH CARE SERVICES

Security Awareness, Understanding & Accountability Form

(External Entity Version 1.0)

Exhibit F

Annual Information Security Training and Awareness is required for any person that is required to use California Correctional Health Care Services (CCHCS) IT assets or information as part of their job functions or assigned tasks. By signing this document you certify that you are aware of, understand, and are accountable for complying with CCHCS Information Security Policies as defined in the California Department of Corrections & Rehabilitation (CDCR) Department Operations Manual (DOM).

NAME:	ORGANIZATION:	
TELEPHONE NUMBER:	E-MAIL ADDRESS:	
HAS COMPLETED INFORMATION SECURITY TRAINING AND AWARENESS	Yes	DATE:

As a user of CCHCS IT assets or information, I agree to the following terms and conditions:

a. I will comply with all State policies and laws regarding the access, use and protection of State IT assets and information.
b. I will comply with all CCHCS Information Security Policies as defined in the CDCR DOM, Chapter 4, Article 45.
c. I will access or use CCHCS IT assets and information for authorized purposes only.
d. I will exercise all precautions necessary to protect confidential, sensitive, personal, and protected information I access or use.
e. I will use care to physically secure CCHCS IT assets and information from unauthorized access, theft, damage, or misuse.
f. I will not share my passwords with anyone.
g. I will only access system areas, functions, or files that I am formally authorized to use.
h. I will access CCHCS systems and networks using only my assigned user ID(s) and password(s).
i. I will not perform any act that interferes with the normal operations of IT systems.
j. I will use only CCHCS approved IT systems.
k. I will comply with all applicable copyright laws.
l. I have taken within this current calendar year or will take within the next 30 business days the CCHCS Information Security Awareness Training and understand my responsibilities as described in that material.
m. I acknowledge my responsibility to take the CCHCS Information Security Awareness Training at least annually thereafter or as directed by CCHCS.
n. I understand that illegal use of CCHCS IT assets and information may be a public offense punishable under Section 502 of the California Penal Code.

NAME: (PRINT NAME)	SIGNATURE:	DATE SIGNED
MANAGER: (PRINT NAME)	MANAGER'S SIGNATURE:	DATE SIGNED

State of California
California Correctional Health Care Services (CCHCS/CDCR)

Non Redisclosure Agreement ("NRDA")

This NRDA is entered into this day _____ month _____ year 20__ between CCHCS/CDCR (Discloser) and _____, ("Individual") an individual providing services through a Memorandum of Understanding number ___20-00086_____ ("MOU") (between California Correctional Health Care Services (CCHCS/CDCR) and County of __El Dorado_____("County") through the term of the Agreement.

WHEREAS Discloser possesses certain information relating to CCHCS/CDCR that is confidential and proprietary to Discloser (hereinafter referred to as "confidential information"); and

WHEREAS the Individual is willing to receive disclosure of the confidential information pursuant to the terms of this Agreement in performing duties for the purpose of assisting County in fullfiling its obligations under the MOU through access via a secure electronic file transfer site hosted by CCHCS/CDCR through the term of the above MOU;

NOW THEREFORE, in consideration for the mutual undertakings of the Discloser and the County where Individual will access and use the confidential information as outlined in the MOU, the Individual understands and agrees to the following:

1. Disclosure. Discloser agrees to disclose and Individual agrees to receive confidential information while performing duties for the purpose of assisting the County in fulfilling its obligations under the MOU.

2. Confidentiality. All Individuals will comply with all federal and state privacy laws regarding personally identifiable information ("PII") and protected health information ("PHI"). Entrance to any CCHCS/CDCR facility requires Individual signature of this NRDA before being allowed access to any CCHCS/CDCR hosted website, server or file respository or commencing work. Failure to sign this NRDA is grounds for Individual to be refused issuance of access credentials (i.e. username and password), or refusual to commence work.

2.1 No Use. Individual agrees not to use the confidential information in any way, or to manufacture or test any content embodying confidential information, except for the purpose set forth above or by the MOU.

2.2 No Disclosure. Individual agrees to abide by all federal and state laws to prevent and protect the confidential information, or any part thereof, from disclosure to any person other than other authorized Individuals (authorized

users identified and approved by the County in writing) or CDCR/CCHCS employees having a need for disclosure in connection with Individual's authorized use of the confidential information.

3. Limits on Confidential information. Confidential information shall not be deemed proprietary and the Individual shall have no obligation with respect to such information where the information:

3.1. Was known to Individual prior to receiving any of the confidential information from Discloser;

3.2. Has become publicly known through no wrongful act of Individual or others;

3.3. Was received by Individual without breach of this NRDA from a third party without restriction as to the use and disclosure of the confidential information;

3.4. Was independently developed by Individual without use of the confidential information; or

3.5. Was ordered to be publicly released by the requirement of an authorized government agency.

4. Ownership of Confidential information. Individual agrees that all confidential information shall remain the property of Discloser, and that Discloser may use such confidential information for any purpose without obligation to Individual. Nothing contained herein shall be construed as granting or implying any transfer to Individual of rights, patents, or other intellectual property protecting or relating to confidential information.

5. Term and Termination. The obligations of this NRDA shall continue for the duration of the MOU to which this NRDA was executed, and unless and until the confidential information disclosed to Individual is no longer confidential.

6. Survival of Rights and Obligations. This NRDA is binding and enforceable to and by (a) the Discloser, its successors, and assignees; and (b) Individual, its successors and assignees.

IN WITNESS WHEREOF, the undersigned Individual and CCHCS have executed this agreement effective as of the date above.

Signature: _____
(Individual)

Signature: _____
(CCHCS – Chief Privacy Officer)

Note to County Approver/Authorizer: This NRDA, once executed, shall be maintained with the MOU file and copies shall be made available and provided to CCHCS on request.