Memorandum of Understanding
18MOU-BCIIS-CURES-XXX

Controlled Substance Utilization Review and Evaluation System (CURES) Information Exchange Web Service

BETWEEN

California Department of Justice
California Justice Information Services Division
Bureau of Criminal Identification and Investigative Services (BCIIS), CURES

AND

Insert Name of Entity

FOR OFFICIAL USE ONLY

October 2018

Version No.: 1.0

1. Background

The Controlled Substance Utilization Review and Evaluation System (CURES) is a database containing information about Schedule II, III, and IV controlled substance prescriptions dispensed to patients, as reported by the dispensing pharmacy, clinic, or other dispenser pursuant to Health and Safety Code section 11165(d). The CURES Program grants authorized health care practitioners and pharmacists access to query the CURES database to assist them in their efforts to ensure appropriate prescribing, ordering, administering, furnishing, and dispensing of controlled substances.

Assembly Bill 40 requires the Department of Justice to establish a method of system integration whereby approved health care practitioners and pharmacists may use a qualified health information technology system to access information in the CURES database. As a prerequisite to system integration, each entity that operates a heath information technology system must certify that it has entered into a memorandum of understanding with the California Department of Justice (DOJ) addressing the technical specifications of the system to ensure the security of CURES data in the CURES database and the secure transfer of CURES data from the CURES database.

2. Purpose

The California Department of Justice, California Justice Information Services (CJIS) Division, Bureau of Criminal Identification and Investigative Services (BCIIS), Controlled Substance Utilization Review and Evaluation System, referred to collectively herein as “STATE,” and, the entity operating the health information technology system (including its officers, employees, and agents), referred to herein as “ENTITY,” enter into this memorandum of understanding (MOU) in accordance with Assembly Bill 40. Chaptered on October 9, 2017, Assembly Bill 40 is codified in Health and Safety Code section 11165.1, and will be cited accordingly in this MOU. STATE and ENTITY may be collectively referred to herein as the “PARTIES,” and individually referred to as “PARTY.”

Pursuant to Health and Safety Code (HSC) section 11165.1(a)(1)(E), an approved health care practitioner or pharmacist may submit queries to the CURES database through a health information technology (HIT) system if the entity that operates the HIT system can certify all of the following:

(i) The entity will not use or disclose CURES data for any purpose other than delivering the CURES data to an approved health care practitioner or pharmacist or performing data processing activities that may be necessary to enable the delivery unless authorized by, and pursuant to, state and federal privacy and security laws and regulations.
(ii) The HIT system will authenticate the identity of an authorized health care practitioner or pharmacist initiating queries to the CURES database and, at the time of the query to the CURES database, the HIT system submits the following data regarding the query to CURES:
(I) The date of the query.
(II) The time of the query.
(III) The first and last name of the patient queried.
(IV) The date of birth of the patient queried.
(V) The identification of the CURES user for whom the system is making the query.
(iii) The HIT system meets applicable patient privacy and information security requirements of state and federal law.

(iv) The entity has entered into an MOU with the department that solely addresses the technical specifications of the HIT system to ensure the security of the CURES data in the CURES database and the secure transfer of CURES data from the CURES database. The technical specifications shall be universal for all HIT systems that establish a method of system integration to retrieve CURES data from the CURES database. The MOU shall not govern, or in any way impact or restrict, the use of CURES data received from the CURES database or impose any additional burdens on covered entities in compliance with the regulations promulgated pursuant to the federal Health Insurance Portability and Accountability Act of 1996 found in Parts 160 and 164 of Title 45 of the Code of Federal Regulations.

Consistent with Health and Safety Code section 11165.1(a)(1)(E), the objective of this MOU is to address the technical specifications of the HIT system to ensure the security of the CURES data in the CURES database and the secure transfer of CURES data from the CURES database. As used herein, the term “MOU” shall be understood to include this document and all exhibits identified in Paragraph 8.

STATE’s method of system integration developed to meet the requirements of Assembly Bill 40 shall be referred to in this MOU as the “CURES Information Exchange Web Service.”

“CURES data,” as such term is used in this MOU, shall include:

(i) Information reported to the Department of Justice by dispensing pharmacies, clinics, or other dispensers pursuant to Health and Safety Code section 11165(d); and,

(ii) All Sensitive Information and Personal Information, as those terms are defined in Exhibit E, obtained by a health information technology system, or the entity that operates it, from the Department of Justice through the CURES Information Exchange Web Service.

3. Services and Responsibilities

A. ENTITY will be responsible for complying with all requirements described in this Paragraph 3.A. By signing the MOU, ENTITY certifies, warrants, and represents its compliance with these requirements. ENTITY shall immediately notify STATE if, at any point during the Term, ENTITY fails to comply or is unable to maintain compliance with any requirement described in this Paragraph 3.A.

i. Certifying compliance, and maintaining compliance throughout the duration of this MOU, with Health and Safety Code section 11165(a)(1)(E)(i), which prohibits ENTITY from using or disclosing CURES data received from the CURES database for any purpose other than delivering the CURES data to an approved health care practitioner or pharmacist or performing data processing activities that may be necessary to enable the delivery unless authorized by, and pursuant to, state and federal privacy and security laws and regulations.

ii. Certifying compliance, and maintaining compliance throughout the duration of this MOU, with Health and Safety Code section 11165(a)(1)(E)(ii), which contains two distinct requirements.

a. The HIT system is required to authenticate the identity of an authorized health care practitioner or pharmacist initiating queries to the CURES database. This is a requirement that the HIT system operated by ENTITY verify the identification of the health care practitioner or pharmacist initiating the query, or on whose behalf the HIT system is initiating the query. For purposes of complying with this requirement, there can only be one health care practitioner or pharmacist identified with each query.

b. The HIT system is required to submit the following data regarding the query to CURES at the time of the query:

- The date of the query.
- The time of the query.
- The first and last name of the patient queried.
- The date of birth of the patient queried.
- The identification of the authorized health care practitioner or pharmacist for whom the system is making the query. For purposes of complying with this requirement, there can only be one health care practitioner or pharmacist identified with each query.

iii. Submitting to CURES a notification confirming receipt of the CURES data by the health care practitioner or pharmacist identified in Paragraph 3.A.ii. For purposes of complying with this requirement, there can only be one health care practitioner or pharmacist identified with each query, and the submissions required by Paragraph 3.A.ii and 3.A.iii must reflect the same individual. If ENTITY cannot comply with this requirement at commencement of the Term, then ENTITY must submit with the MOU a plan, including a detailed timeframe, for becoming compliant with this requirement.

iv. Ensuring compliance of its HIT system with the format standards specified in the most current CURES Information Exchange Web Service Implementation Guide, which may be periodically updated by STATE, located on the CURES web page at www.oag.ca.gov/cures/iews.

v. Certifying that ENTITY is either a “covered entity” or “business associate,” as such terms are defined in the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 17931 et seq., and its implementing regulations found in Parts 160 and 164 of Title 45 of the Code of Federal Regulations, with respect to any CURES data its HIT system receives from STATE through the CURES Information Exchange Web Service.

vi. Certifying compliance, and maintaining compliance throughout the duration of this MOU, with Health and Safety Code section 11165(a)(1)(E)(iii), which requires the HIT system to meet applicable patient privacy and information security requirements of state and federal law, including, but not limited to, the regulations promulgated pursuant to the federal Health Insurance Portability and Accountability Act of 1996 found in Parts 160 and 164 of Title 45 of the Code of Federal Regulations.

vii. Certifying compliance, and maintaining compliance throughout the duration of this MOU, with Health and Safety Code section 11165(a)(1)(E)(iv), which, as a condition precedent to system integration, requires ENTITY to enter into and maintain an active MOU with STATE that addresses the technical specifications of the HIT system to ensure the security of the CURES data in the CURES database and the secure transfer of CURES data from the CURES database.

viii. Timely payment of fees, as provided in EXHIBIT D, associated with establishing and maintaining integration with the CURES database pursuant to Health and Safety Code section 11165(a)(1)(H).

ix. Compliance with all terms, provisions, and exhibits of this MOU.

B. STATE will be responsible for complying with all requirements described in this Paragraph 3.B.

i. Verifying that health care practitioners and pharmacists who submit queries to the CURES database through a HIT system, or on whose behalf a HIT system submits queries, are authorized or approved CURES users. As used herein, the terms “authorized” or “approved,” when used to describe health care practitioners, pharmacists, or subscribers, shall mean those health care practitioners or pharmacists who have submitted an application to and been approved by the Department of Justice for access to CURES data pursuant to Health and Safety Code section 11165.1(a)(1)(A).

ii. Prohibiting, suspending, or terminating integration with an ENTITY and its respective HIT system(s) if at any time during this MOU such ENTITY (including any officer, employee or agent of ENTITY) fails to meet the requirements of Paragraph 3.A of this MOU.

iii. Transmitting CURES data to ENTITY in a manner consistent with EXHIBIT C.

4. Responsible Parties

For STATE:

Name, Title, Agency	Role
Joe Dominic, Chief, California Justice Information Services Division, Department of Justice	Division Chief/Executive Officer
Jenny Reich, Bureau Director, Bureau of Criminal Identification and Investigative Services, Department of Justice	Executive Sponsor
Audra Opdyke, Assistant Bureau Director, Department of Justice	Business Sponsor/BCIIS
Tina Farales, Staff Services Manager II, Department of Justice	Business Manager/CURES Program

Rodney Smith, Bureau Director, Application Development Bureau	Bureau IT Project Sponsor
Todd Ibbotson, Information Security Officer	Bureau IT Project Sponsor
Bhaskar Rudrakshala, Information Technology Manager I	CURES IT Manager

For ENTITY:

Name, Title, Agency	Role	Business Address	Phone/Email

5. Term of Agreement

This MOU will commence on the date it is fully executed by all PARTIES, as established by the latest signature date, and expire on June 30, 2022, which shall constitute the “Term.” This MOU will be reviewed 90 days prior to the end of the Term to renew and/or evaluate changes. If renewing, a new MOU with updated signatures and current dates will be required. During the Term, STATE may amend this MOU pursuant to Paragraph 7, and the PARTIES may terminate this MOU pursuant to EXHIBIT B.

6. Notices

All notices hereunder may be sent by U.S. certified or registered mail, postage prepaid, return receipt requested, or by Federal Express or other overnight courier which obtains a signature upon delivery for next business day delivery, or by hand delivery, or electronic mail provided that a copy is also sent on the same day by one of other the methods set forth above, with a copy to follow addressed to such PARTY at the address of such PARTY set forth below or at such other address as such PARTY shall designate from time to time by notice:

If to STATE:

CURES Program
P.O. Box 160447
Sacramento, CA 95816
Attention: CURES Manager
E-mail: cures@doj.ca.gov

If to ENTITY:

Name: ______________________________
Address: ______________________________
____
Attention: ______________________________
E-mail: ______________________________

With a copy to:
(which shall not
constitute notice)

Name: ______________________________
Address: ______________________________
____
Attention: ______________________________
E-mail: ______________________________

Notices shall be deemed served if by electronic mail upon receipt of a transmittal confirmation (if received during normal business hours, otherwise on the next business day) and provided that a copy is sent by U.S. mail, and in the case of overnight courier or hand delivery, on the date actually delivered to or rejected by the intended recipient, except for notice(s) which advise the other PARTY of a change of address of the PARTY sending such notice, which notices shall not be deemed served until actually received by the PARTY to whom such notice(s) are addressed or delivery is refused by such PARTY. Notwithstanding the foregoing provisions of this Paragraph, notices served by hand delivery shall be deemed served on the date of delivery if delivered at or prior to 5:00 P.M. on a business day and on the next business day if delivered after 5:00 P.M. on a business day or at any time on a non-business day.

7. Amendments

STATE shall have the express unilateral right to change or add any provisions, terms, or conditions of or to this MOU. The types of changes may include, but shall not be limited to, updated security requirements or formats and/or versions of technical data/processes associated with HIT system integration.

STATE shall provide to ENTITY advance written notice prior to amendments made to the MOU. For non-technical changes, STATE shall provide no less than thirty (30) days advance written notice. For technical changes, STATE shall provide no less than ninety (90) days advance written notice. Notice shall be provided to ENTITY in the manner prescribed by Paragraph 6. ENTITY shall execute and return to STATE any amendment to the MOU issued by STATE within fifteen (15) calendar days from receipt thereof (as determined by the notice provisions of Paragraph 6 of the MOU). Failure of ENTITY to timely execute and return to STATE any amendment to the MOU issued by STATE shall constitute a violation of Paragraph 3.A., and STATE may, as a result, terminate the ability of ENTITY and its HIT system to retrieve data from through the CURES Information Exchange Web Service.

No amendment or variation of the terms of this MOU shall be valid unless made in writing and pursuant to this paragraph. No oral understanding or agreement not incorporated in the MOU is binding on any of the PARTIES.

8. Exhibits

All applicable exhibits are included with this MOU. ENTITY agrees to accept and abide by the requirements outlined in each exhibit.

List of Exhibits

EXHIBIT A. Special Terms and Conditions

EXHIBIT B. Miscellaneous Provisions

EXHIBIT C. CURES Information Exchange Web Service Implementation Overview

EXHIBIT D. Fees and Payment

EXHIBIT E. Confidentiality and Information Security Requirements

This MOU may be executed in one or more counterparts, and with counterpart e-mail signature pages, each of which shall be deemed an original, but all of which when taken together shall constitute one and the same instrument.

STATE and ENTITY warrant that each has full power and authority to enter into and perform this MOU, and that the person signing this MOU for each PARTY has been properly authorized and empowered to enter into this MOU on behalf of such PARTY.

IN WITNESS WHEREOF, the parties hereto have executed this MOU on the day and year as indicated:

Joe Dominic, Chief
Department of Justice
California Justice Information Services Division

Date

Jenny Reich, Bureau Director
Department of Justice
California Justice Information Services Division
Bureau of Criminal Identification and Investigative Services

Date

Rodney Smith, Bureau Director
Department of Justice
California Justice Information Services Division
Application Development Bureau

Date

Todd Ibbotson, Information Security Officer
Department of Justice
California Justice Information Services Division

Date

Date

Date

EXHIBIT A
SPECIAL TERMS AND CONDITIONS

1. Employee Access to Information

The entity will not use or disclose CURES data for any purpose other than delivering the CURES data to an approved health care practitioner or pharmacist or performing data processing activities that may be necessary to enable the delivery unless authorized by, and pursuant to, state and federal privacy and security laws and regulations.

2. Data Fidelity

STATE does not independently verify the accuracy of the CURES data in the CURES database. The CURES database contains Schedule II, Schedule III, and Schedule IV prescription information reported by California licensed pharmacies and direct dispensers, and is therefore only as accurate as the information provided by these entities.

3. Safeguard Review

During the term of this MOU, STATE may require ENTITY to provide information to STATE demonstrating its use of CURES data complies with the Health Insurance Portability and Accountability Act of 1996.

4. Maintenance of an Active CURES User Account

It shall be the responsibility of healthcare practitioners and pharmacists to verify through the CURES portal that their CURES account profiles are current, which shall include, at a minimum, completion of the annual update, and that they possess active CURES accounts. The failure of healthcare practitioners and pharmacists to complete the annual update or maintain an active CURES account status will result in rejection of their queries.

EXHIBIT B
MISCELLANEOUS PROVISIONS

1. Applicable Law

This MOU shall be governed by and shall be interpreted in accordance with the laws of the State of California; venue of any action brought with regard to this MOU shall be in Sacramento County, Sacramento, California.

2. Termination

A. Right to Terminate.
   - i. For convenience. ENTITY shall have the right to terminate this MOU if it determines that termination is in its interest.
   - ii. For cause. Either PARTY may terminate this MOU if the PARTY determines the other PARTY is not in compliance with Paragraph 3 of the MOU.

B. Notice of Termination. A PARTY shall terminate this MOU by delivering to the other PARTY a Notice of Termination specifying the termination and the effective date thereof. If the termination is "for cause," the Notice of Termination shall include a statement of that cause.

C. Responsibilities of the PARTIES on the effective date of termination.
   - i. STATE shall terminate the ability of ENTITY and its HIT system to retrieve CURES data from the CURES database.
   - ii. ENTITY shall be responsible for all fees accrued on or before the effective date of the termination, pursuant to EXHIBIT D.
   - iii. ENTITY shall maintain continuing obligations under the terms of this MOU, notwithstanding the termination or expiration thereof, with respect to any CURES data retained by ENTITY or its HIT system.

3. Indemnification

ENTITY agrees to indemnify, defend and save harmless STATE, its officers, agents and employees from any and all third party claims, costs (including without limitation reasonable attorneys' fees), and losses due to the injury or death of any individual, or the loss or damage to any real or tangible personal property, resulting from the violation of any state or federal privacy or security law or regulation applicable to ENTITY'S use of CURES data, the willful misconduct or negligent acts or omissions of ENTITY or any of its affiliates, agents, subcontractors, employees, or officers in connection with the performance of this MOU. Such defense and payment will be conditional upon the following:

A. STATE will notify ENTITY of any such claim in writing and tender the defense thereof within a reasonable time; and

B. ENTITY will have sole control of the defense of any action on such claim and all negotiations for its settlement or compromise; provided that (i) when substantial principles of government or public law are involved, when litigation might create precedent affecting the future STATE operations or liability, or when involvement of STATE is otherwise mandated by law, STATE may participate in such action at its own expense with respect to attorneys' fees and costs (but not liability; (ii) where a settlement would impose liability on STATE, affect principles of California government or public law, or impact the authority of STATE, STATE will have the rights to approve or disapprove any settlement or compromise, which approval will not unreasonably be withheld or delayed; and (iii) STATE will reasonably cooperate in the defense and in any related settlement negotiations.

4. Confidentiality of Data

CURES data shall be protected by ENTITY from unauthorized use and disclosure through the observance of the provisions of this MOU and applicable state and federal laws and regulations including, but not limited to, the Health Insurance Portability and Accountability Act of 1996.

5. News Releases

Unless otherwise exempted, news releases, endorsements, advertising, and social media content pertaining to this MOU shall not be made without prior written approval of STATE.

6. Change Management Process

ENTITY agrees to notify STATE in advance of any changes associated with this MOU or access to the CURES data that will affect or impact the technical environment of the HIT system, including, but not limited to, technical or system changes involving major modifications to infrastructure or disconnection from the CURES database by ENTITY, and modifications to agreed upon configurations or outages. Contacts for such notification are listed in Paragraph 6 (Notices) of the MOU.

7. Issue Resolution Procedures

If ENTITY or STATE has a concern regarding the services, deliverables, invoicing, or MOU terms and conditions which cannot be informally resolved, ENTITY or STATE will document its concern and advise the responsible parties. Once an issue has been identified, a meeting will take place within thirty (30) calendar days, between ENTITY and STATE to discuss and resolve the issue. If the dispute persists, ENTITY shall submit to STATE Division Chief or designee a written demand for a final decision regarding the disposition of any dispute between the PARTIES arising under, related to or involving this MOU. ENTITY's written demand shall be fully supported by factual information. STATE Division Chief or designee shall have 30 days after receipt of ENTITY's written demand invoking this Paragraph (Disputes) to render a written decision. Contacts for such notification are listed in Paragraph 6 (Notices) of the MOU. In the event of an unresolved issue, ENTITY and STATE agree that they will continue to carry out all their MOU responsibilities that are not affected by the issue.

EXHIBIT C

California Department of Justice
CURES Information Exchange Web Service
Overview

October 2018

EXHIBIT C

The purpose of this document is to provide an overview of the CURES Information Exchange Web Service. Outlined below is a brief explanation of the technology, as well as the use cases, associated with this web service.

The CURES Program will provide systems integration with the Health Information Technology (HIT) community through RESTful web services. For the initial phase, the following web services will be available to serve the following functions:

- Searches for a patient for a given timeframe
- Retrieves a patient controlled substance history
- CURES and a HIT system's user account status
- Notification confirming receipt of CURES data by the health care practitioner or pharmacist who submitted the query

Information will be exchanged using NCPDP SCRIPT XML REST-based format. Searches can be executed for a period using partial or exact match modes.

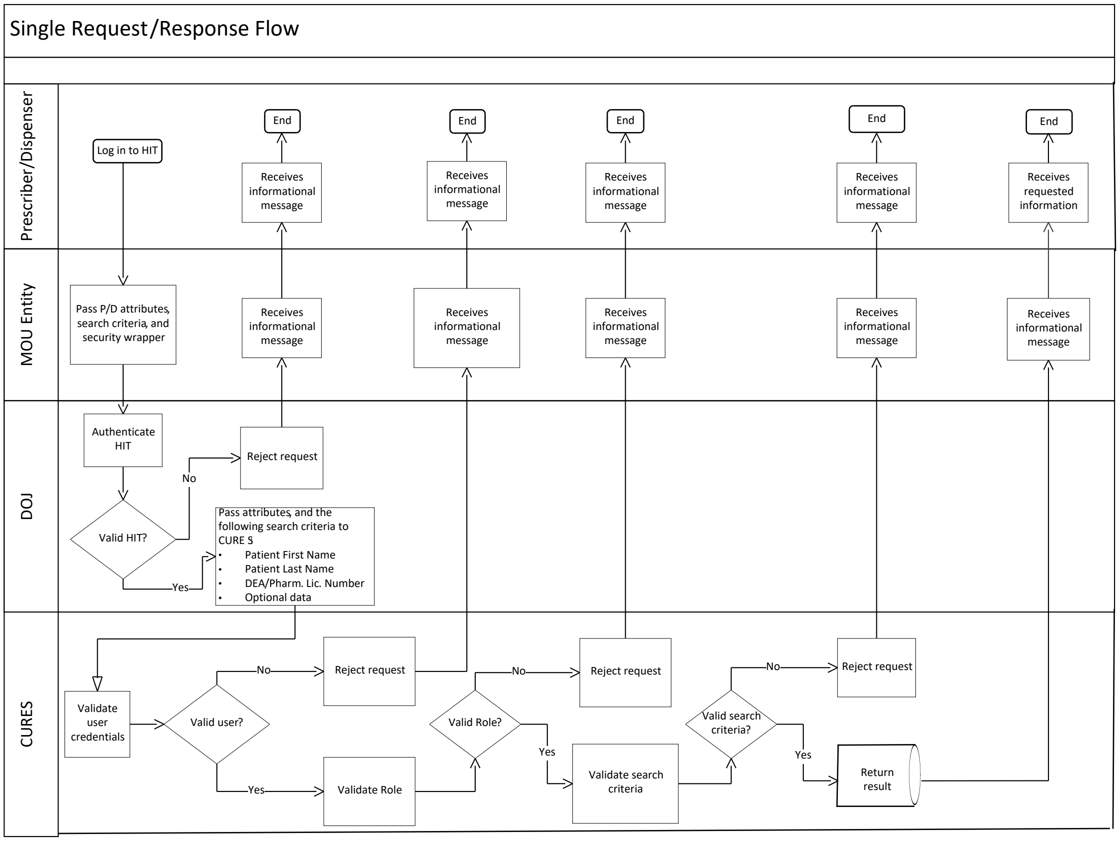
EXHIBIT C

Search Patient and Generate Report

The CURES web service will support two patient search use cases:

- Query Use Case 1 – Single Request/Response
    - Use Case 1 follows the NCPDP standard where every search patient request returns either no match or a single match. The result will be either an error message stating there is no match, or will return all of the prescription history associated to the matched entity.

Figure 1 – Single Request/Response


Single Request/Response Flow
Prescriber/Dispenser
MOU Entity
DOJ
CURES
Log in to HIT
End
Receives informational message
End
Receives informational message
End
Receives informational message
End
Receives informational message
End
Receives requested information
Pass P/D attributes, search criteria, and security wrapper
Receives informational message
Receives informational message
Receives informational message
Receives informational message
Receives informational message
Authenticate HIT
Valid HIT?
No
Reject request
Yes
Pass attributes, and the following search criteria to CURES
• Patient First Name
• Patient Last Name
• DEA/Pharm. Lic. Number
• Optional data
Validate user credentials
Valid user?
No
Reject request
Yes
Validate Role
Valid Role?
No
Reject request
Yes
Validate search criteria
Valid search criteria?
No
Reject request
Yes
Return result

Prescriber Attributes

1) First Name
2) Last Name
3) DEA #

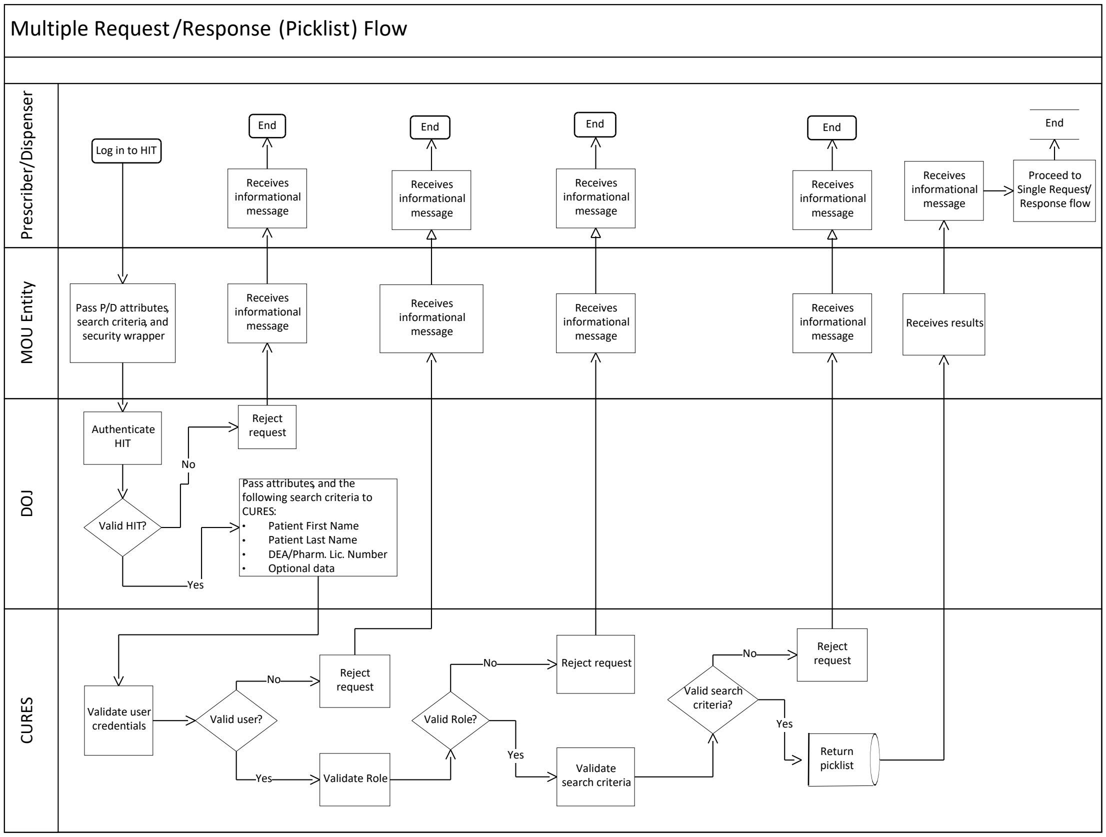
Dispenser Attributes

1) First Name
2) Last Name
3) Pharmacist Lic. #

EXHIBIT C

- Query Use Case 2 – Multiple Matches (Picklist)
    - Use Case 2 supports multiple matches, via a pick list. In this use case, a patient search returns multiple entities using a NCPDP-like message structure. The requesting entity would then send one or multiple single requests to retrieve the prescription history associated to the matched entity.
    - For those HIT systems that cannot support this functionality, a response message redirecting the health care practitioner/pharmacist to the CURES web application is returned.

Figure 2 – Multiple Request/Response


Multiple Request /Response (Picklist) Flow
Prescriber/Dispenser
MOU Entity
DOJ
CURES
Log in to HIT
End
End
End
End
End
Receives informational message
Receives informational message
Receives informational message
Receives informational message
Receives informational message
Proceed to Single Request/ Response flow
Pass P/D attributes, search criteria, and security wrapper
Receives informational message
Receives informational message
Receives informational message
Receives informational message
Receives results
Authenticate HIT
Reject request
No
Valid HIT?
Yes
Pass attributes, and the following search criteria to CURES:
• Patient First Name
• Patient Last Name
• DEA/Pharm. Lic. Number
• Optional data
Validate user credentials
Valid user?
No
Yes
Reject request
Validate Role
Valid Role?
No
Yes
Reject request
Validate search criteria
Valid search criteria?
No
Yes
Reject request
Return picklist

Prescriber Attributes

1) First Name
2) Last Name
3) DEA #

Dispenser Attributes

1) First Name
2) Last Name
3) Pharmacist Lic #

EXHIBIT C

Account Status Check

In addition to the query use cases, the CURES web services will provide web services to query for account status. The first allows the HIT systems to query for the CURES user account status. The second allows the HIT systems to query for their own account status. These services allow the HIT systems to troubleshoot and alter process flows based on account status.

Audit Patient Activity Report

HIT systems are required to submit a notification confirming the receipt of CURES data by the health care practitioner or pharmacist who submitted the query. For purposes of complying with this requirement, there can be only one health care practitioner identified with each query, and, the health care practitioner or pharmacist receiving the CURES data must be the health care practitioner or pharmacist who submitted the initial query.

Figure 3 – Audit Patient Activity Report

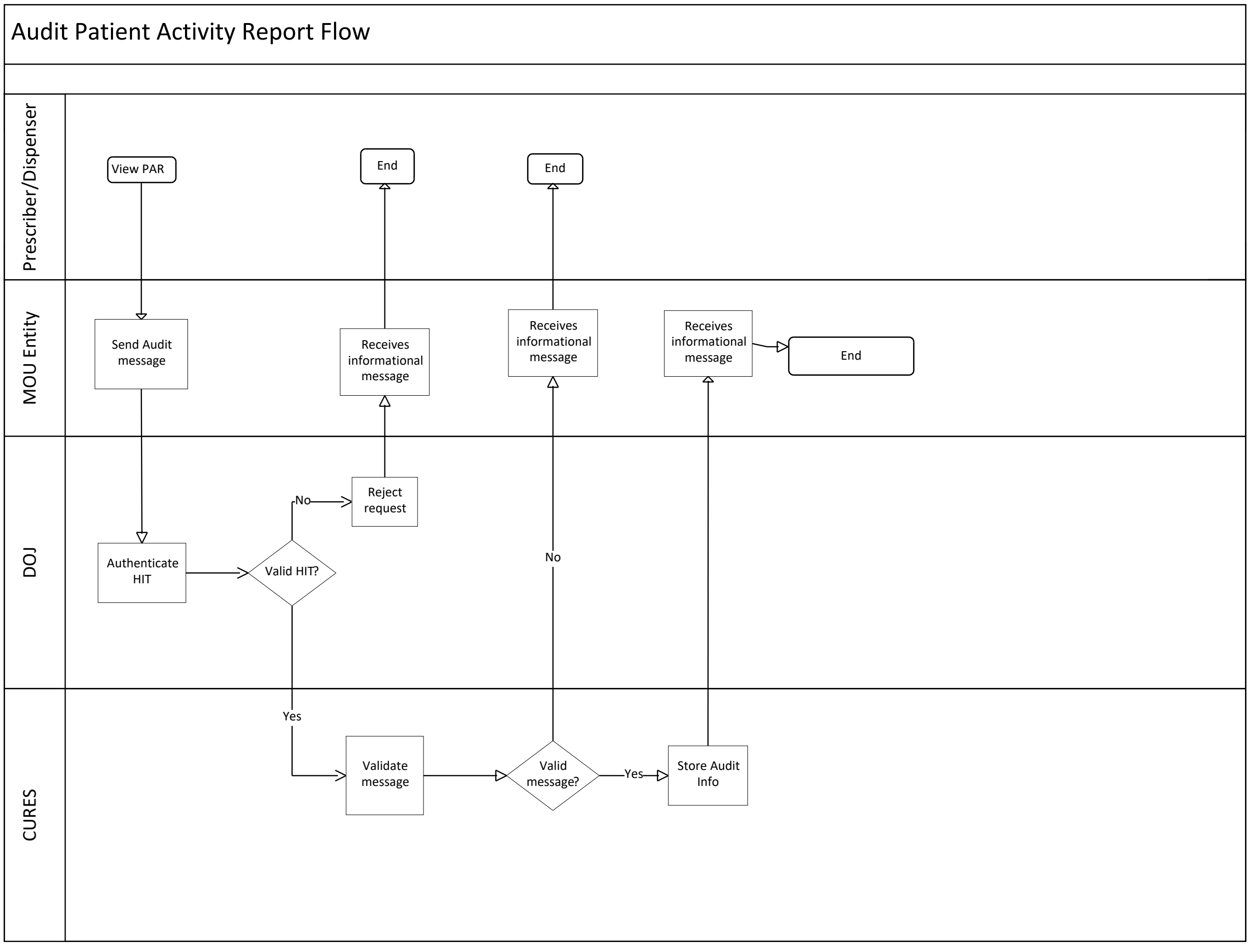
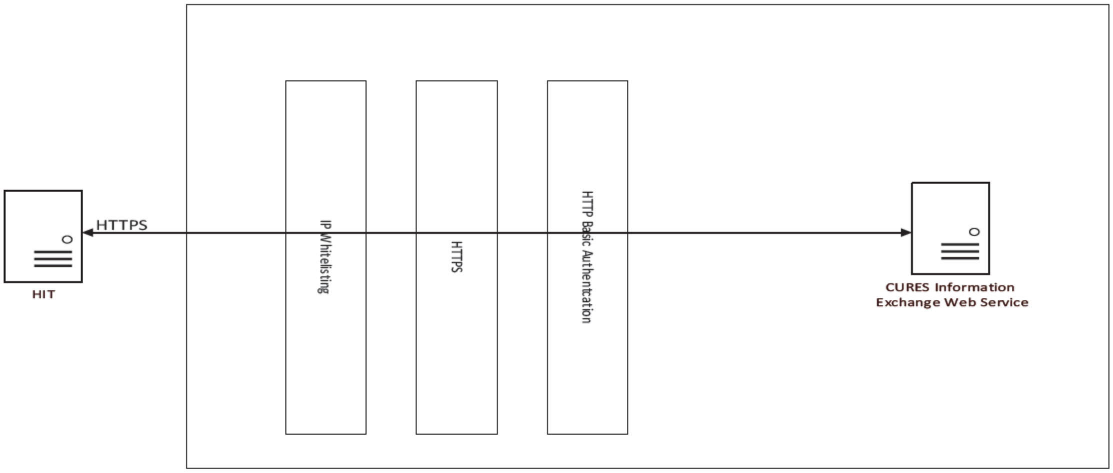


EXHIBIT C

Security

The CURES web service has three layers of security. Each layer is built on top of the previous to ensure the secure exchange of information. Each REST endpoint is stateless, resulting in every request going through all three layers.

Figure 4 – Security Layers


HTTPS
HIT
IP Whitelisting
HTTPS
HTTP Basic Authentication
CURES Information Exchange Web Service

Network Security

IP whitelisting will ensure only enrolled HIT systems can communicate with the CURES web service.

Communication Security

Communication between the CURES web service and the HIT systems will be over the Internet. As a result, Transport Layer Security (TLS) is required to ensure secure communication between CURES Web services and HIT.

Access Security

After entering into an MOU with the Department of Justice, HIT systems will be provisioned with a CURES web service account. Every RESTful web services request should be accompanied with the credentials and will be validated to ensure the account is valid and in good standing.

EXHIBIT D
FEES AND PAYMENT

Pursuant to Health and Safety Code section 11165.1(a)(1)(H), an entity that operates a HIT system "that is requesting to establish integration with the CURES database shall pay a reasonable fee to cover the cost of establishing and maintaining integration with the CURES database."

1. Fee to Establish Integration (Connectivity Fee)

The Connectivity Fee is a mandatory, one-time, on-boarding fee to cover the cost of connecting ENTITY's HIT system to the CURES Information Exchange Web Service, and is a condition to such integration. The Connectivity Fee amount is fifteen hundred dollars ($1,500). The Connectivity Fee is due with ENTITY's signed memorandum of understanding (MOU). If STATE does not approve ENTITY's MOU, the Connectivity Fee shall be returned to ENTITY. The Connectivity Fee must be paid by check, made payable to the California Department of Justice.

2. Fee to Maintain Integration (Maintenance Fee)

The Maintenance Fee is a mandatory annual fee to cover the cost of maintaining ENTITY's HIT system integration with the CURES Information Exchange Web Service. The Maintenance Fee shall be the established rate multiplied by the number of healthcare practitioners and pharmacists who utilize the CURES Information Exchange Web Service through ENTITY's HIT system. The rate shall be established on an annual basis by STATE. STATE projects the rate to be between five dollars ($5) and twenty dollars ($20) per healthcare practitioner or pharmacist, but this merely reflects an approximation and represents neither a ceiling nor a floor. A healthcare practitioner or pharmacist shall be deemed to have used the CURES Information Exchange Web Service if he or she submits one or more queries through the HIT system during the applicable period.

The Maintenance Fee shall represent a prepayment by ENTITY for its use of the CURES Information Exchange Web Service in the applicable fiscal year. The due date for payment of the Maintenance Fee shall depend upon whether ENTITY is requesting commencement or continuation of HIT system integration with the CURES Information Exchange Web Service.

A. ENTITY Year One Maintenance Fee

For an ENTITY operating a HIT system initially requesting integration with the CURES Information Exchange Web Service, that is paying its first Maintenance Fee, the Maintenance Fee shall be due with submission of its signed MOU. Payment of the Maintenance Fee is a condition of integration. The Maintenance Fee for an ENTITY commencing integration shall be pro-rated based upon the date that such ENTITY submits its signed MOU to STATE. The proration shall be in quarterly brackets, aligned with the fiscal year (which reflects STATE's billing cycle), as depicted in the below table.

Quarter	Date Range	Proration
1	July 1 – Sept. 30	fee × 1.0
2	Oct. 1 – Dec. 31	fee × 0.75
3	Jan. 1 – Mar. 31	fee × 0.50
4	Apr. 1 – June 30	fee × 0.25

ENTITY shall calculate the Maintenance Fee for the first fiscal year of ENTITY's use based on the estimated number of healthcare practitioners and pharmacists that will utilize the CURES Information Exchange Web Service in the initial fiscal year multiplied by the established Maintenance Fee rate. The Maintenance Fee must be paid by check, made payable to the California Department of Justice. A "true-up" process, described in Paragraph 2.C, will reconcile any difference between the estimated number of fiscal year one users and the actual number of users during the applicable fiscal year. There is no proration after fiscal year one.

Example

Fiscal Year	Date MOU Signed/Submitted	Fiscal Quarter	Sample Maintenance Fee Rate	Estimated Users from Onboarding Questionnaire	Calculation	Proration	**Due**
1	Nov. 15, 2020	Q2	$15	100	$15×100=$1,500	$1,500×0.5	$750

(Note: For ENTITIES that establish connection prior to June 30, 2019, the Maintenance Fee will be waived for the period up to June 30, 2019.)

B. ENTITY Year Two (and Thereafter) Maintenance Fee

STATE shall calculate the Maintenance Fee for the second fiscal year, and thereafter, based on ENTITY's actual number of healthcare practitioners and pharmacists that utilized the CURES Information Exchange Web Service in the prior applicable fiscal year multiplied by the established Maintenance Fee rate. A "true-up" process, described in Paragraph 2.C, will reconcile any difference between the number of users in the prior fiscal year and the actual number of users in the applicable fiscal year.

For the second fiscal year, and thereafter, STATE shall invoice ENTITY for the Maintenance Fee. Such invoice shall be sent to ENTITY in a manner consistent with the notice provisions of Paragraph 6 of the MOU. ENTITY shall pay to STATE the invoiced Maintenance Fee within forty-five (45) days receipt thereof. The Maintenance Fee must be paid by check, made payable to the California Department of Justice. Timely payment of the Maintenance Fee is a condition of continued integration.

C. Maintenance Fee True-Up Process

Maintenance Fees are calculated using the actual number of users in the preceding fiscal year (except for fiscal year one, where ENTITY estimates the number of users for that year). The "true-up" is a process whereby STATE reconciles any discrepancies between the projected number of users and actual number of users for each fiscal year. The true-up occurs after the close of each applicable fiscal year, such that STATE can ascertain the actual number of users during that fiscal year.

If an ENTITY's actual number of users at the close of a fiscal year is fewer than the preceding fiscal year, which was used by STATE to calculate the Maintenance Fee, STATE shall deduct from the subsequent Maintenance Fee an amount equivalent to the difference in the number of actual users multiplied by the established Maintenance Fee rate.

Conversely, if an ENTITY's actual number of users at the close of a fiscal year is greater than the preceding fiscal year, which was used by STATE to calculate the Maintenance Fee, STATE shall add to the subsequent Maintenance Fee an amount equivalent to the difference in the number of actual users multiplied by by the established Maintenance Fee rate.

EXHIBIT E
CONFIDENTIALITY AND INFORMATION SECURITY REQUIREMENTS

This Confidentiality and Information Security Requirements Exhibit (hereinafter referred to as "this Exhibit") sets forth the information security and privacy requirements the ENTITY is obligated to follow with respect to CURES data pursuant to the MOU. The STATE and ENTITY desire to protect the privacy and provide for the security of CURES data in compliance with state and federal statutes, rules and regulations.

1. Confidentiality of Information.

A. Definitions. The following definitions apply to this Exhibit and relate to STATE Confidential, Sensitive, and/or Personal Information.

i. “The Security Rule,” as defined in 45 CFR Part 160, establishes national standards to protect individuals’’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

ii. Security Rule of 45 CFR Part 164 defines “confidentiality” to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of Protected Health Information. The Security rule also promotes the two additional goals of maintaining the integrity and availability of electronic-Protected Health Information. Under the Security Rule, “integrity” means that e-PHI is not altered or destroyed in an unauthorized manner. “Availability” means that electronic-Protected Health Information is accessible and usable on demand by an authorized person.

iii. “Sensitive Information” is information maintained by the STATE, which is not confidential by definition, but requires special precautions to protect it from unauthorized access and/or modification (i.e., financial or operational information). Sensitive information is information in which the disclosure would jeopardize the integrity of the STATE (i.e., STATE's operations).

iv. “Personal Information” is information, in any medium (paper, electronic, or oral) that identifies or describes an individual (i.e., name, social security number, driver’s license, home/mailing address, telephone number, financial matters with security codes, medical insurance policy number, Protected Health Information, electronic-Protected Health Information etc.) and must be protected from inappropriate access, use or disclosure and must be made accessible to information subjects upon request. It can also be information in the possession of the Department in which the disclosure is limited by law or contractual Agreement (i.e., proprietary information, etc.).

v. Protected Health Information (PHI) is health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations and payment for healthcare services. PHI, or in the case of electronic health information, ePHI, includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage. The information relates to an individual's past, present, and future physical and mental health, the provision of healthcare to an individual, or past, present, and future payments for healthcare. "Protected" means the information is protected under the HIPAA Privacy Rule.

vi. "Breach" is

1. the unauthorized acquisition, access, use, or disclosure of CURES data in a manner which compromises the security, confidentiality or integrity of the information; or
2. the same as the definition of "breach of the security of the system" set forth in 45 CFR 164.402.

vii. "Information Security Incident" is

1. an attempted breach;
2. the attempted or successful unauthorized access or disclosure, modification or destruction of CURES data, in violation of any state or federal law or in a manner not permitted under the MOU including this Exhibit; or
3. the attempted or successful modification or destruction of, or interference with, ENTITY's system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of CURES data.

B. CURES data which may become available to the ENTITY as a result of the implementation of the MOU shall be protected by the ENTITY from unauthorized access, use, and disclosure as described in this Exhibit and consistent with the requirements of the Health Insurance Portability and Accountability Act of 1996.

C. ENTITY is notified that unauthorized disclosure of CURES data may be subject to civil and/or criminal penalties under state and federal law, including but not limited to:

- California Welfare and Institutions Code section 10850
- Information Practices Act 1977- California Civil Code section 1798 et seq.
- California Penal Code Section 502
- Health Insurance Portability and Accountability Act of 1996 ("HIPAA") - 45 C.F.R. § 160.408.
- Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50

2. ENTITY Responsibilities

A. General Rules - Health Insurance Portability and Accountability Act of 1996 ("HIPAA") - 45 CFR Parts 160 and 164

The Security Rule requires ENTITY to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, ENTITY must:

i. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;

ii. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
iii. Protect against reasonably anticipated, impermissible uses or disclosures; and
iv. Ensure compliance by their workforce.

B. Subpoena. If ENTITY receives a subpoena or other validly issued administrative or judicial notice requesting the disclosure of CURES data, ENTITY will immediately notify the STATE Program Contract Manager and the STATE Information Security and Privacy Officer. In no event should notification to STATE occur more than three (3) business days after receipt by ENTITY's responsible unit for handling subpoenas and court orders.

3. Risk Analysis and Management

A. The Administrative Safeguards provisions in the Security Rule require ENTITY to perform risk analysis as part of their security management processes. The risk analysis and management provisions of the Security Rule are addressed separately here because, by helping to determine which security measures are reasonable and appropriate for a particular ENTITY, risk analysis affects the implementation of all of the safeguards contained in the Security Rule.

B. A risk analysis process includes, but is not limited to, the following activities:
i. Evaluate the likelihood and impact of potential risks to e-PHI,
ii. Implement appropriate security measures to address the risks identified in the risk analysis.
iii. Document the chosen security measures and, where required, the rationale for adopting those measures and
iv. Maintain continuous, reasonable, and appropriate security protections.

Risk analysis should be an ongoing process, in which an ENTITY regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI.

4. Administrative Safeguards

A. **Security Management Process**. As explained in the previous section, an ENTITY must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

B. **Security Personnel.** An ENTITY must designate a security official who is responsible for developing and implementing its security policies and procedures.

C. **Information Access Management.** Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires An ENTITY to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).

D. **Workforce Training and Management.** An ENTITY must provide for appropriate authorization and supervision of workforce members who work with e-PHI. An ENTITY must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

E. **Evaluation**. An ENTITY must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

5. Technical Safeguards

A. **Access Control.** An ENTITY must implement technical policies and procedures that allow only authorized persons to access e-PHI.

B. **Audit Controls.** An ENTITY must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

C. **Integrity Controls.** An ENTITY must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

D. **Transmission Security.** An ENTITY must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

E. **ENTITY Responsibilities.** If an ENTITY knows of an activity or practice of ENTITY that constitutes a material breach or violation of ENTITY's obligation, ENTITY must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.

6. Information Security Incidents and/or Breaches

If an ENTITY knows of an activity or practice of ENTITY that constitutes a material breach or violation of ENTITY's obligation, ENTITY must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.

A. **Information Security Incidents and/or Breaches Response Responsibility**. ENTITY shall be responsible for facilitating the Information Security Incident and/or Breach response process as described in 45 CFR 164.308

B. **Discovery and Notification of Information Security Incidents and/or Breaches**. ENTITY shall notify the STATE Program Contract Manager and the STATE Information Security Officer immediately by telephone call and email upon the discovery of the Information Security Incident and/or Breach affecting the security of CURES data if the CURES data was, or is reasonably believed to have been, acquired by an unauthorized person, or there is an intrusion, potential loss, actual loss, or unauthorized use or disclosure of the CURES data is in violation of this MOU, this provision, or applicable state or federal law.

ENTITY shall take:

i. Prompt corrective action to mitigate the risks or damages involved with the Information Security Incident and/or Breach and to protect the operating environment; and
ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

C. **Investigation of Information Security Incidents and/or Breaches**. ENTITY shall promptly investigate such Information Security Incidents and/or Breaches. STATE shall have the right to participate in the investigation of such Information Security Incidents and/or Breaches. STATE shall also have the right to conduct its own independent investigation, and ENTITY shall cooperate fully in such investigations.

D. **Updates on Investigation**. ENTITY shall provide regular (at least once a week) email updates on the progress of the Information Security Incident and/or Breach investigation to the STATE Program Contract Manager and the STATE Information Security Officer until they are no longer needed, as mutually agreed upon between the ENTITY and the STATE Information Security and Privacy Officer.

E. **Written Report**. ENTITY shall provide a written report of the investigation to the STATE Program Contract Manager and the STATE Information Security Officer within 72 hours of the discovery of the Information Security Incident and/or Breach. To the extent ENTITY has such information, the report shall include but not be limited to the following:

i. ENTITY point of contact information;
ii. Description of what happened, including the date of the Information Security Incident and/or Breach and the date of the discovery of the Information Security Incident and/or Breach, if known;
iii. Description of the types of CURES data that were involved and the extent of the information involved in the Information Security Incident and/or Breach;
iv. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed CURES data;
v. A description of where the CURES data is believed to have been improperly transmitted, sent, or utilized;
vi. A description of the probable causes of the improper use or disclosure;
vii. Whether Civil Code sections 1798.82, 45 CFR Part 160 and 164 or any other federal or state laws requiring individual notifications of breaches are triggered; and
viii. Full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the Incident and/or Breach.

F. **Cost of investigation and Remediation.** ENTITY shall be responsible for all costs incurred by STATE due to Information Security Incidents and/or Breaches resulting from ENTITY's failure to perform or from negligent acts of its personnel, and resulting in the unauthorized disclosure, release, access, review, or destruction; or loss, theft or misuse of an information asset. These costs include, but are not limited to, notice and credit monitoring for impacted individuals, STATE staff time, material costs, postage, media announcements, and other identifiable costs associated with the Information Security Incident, Breach and/or loss of data.

VII. Contact Information. To direct communications to the above referenced STATE staff, the ENTITY shall initiate contact as indicated herein. STATE reserves the right to make changes to the contact information below by giving written notice to the ENTITY. Said changes shall not require an amendment to this Exhibit or the MOU.

DOJ Program Manager	**DOJ** **Information Security Officer**
California Department of Justice CURES Program 4949 Broadway Sacramento, CA 95820 Email: CURES@doj.ca.gov Telephone: (916) 210-3187	California Department of Justice Information Security Officer 4949 Broadway Sacramento, CA 95820 Email: dojiso@doj.ca.gov Telephone: (916) 210-5045

DOJ Confidentiality and Security Compliance Statement

CALIFORNIA DEPARTMENT OF JUSTICE
CONFIDENTIALITY AND SECURITY COMPLIANCE STATEMENT v 2018 01

Information resources maintained by the California Department of Justice (DOJ) and provided to your entity may be confidential, sensitive, and/or personal. CURES data is not open to the public and requires special precautions to protect it from wrongful access, use, disclosure, modification, and destruction.

We hereby acknowledge that the confidential and/or sensitive records of the DOJ are subject to strict confidentiality requirements imposed by state and federal law, which may include, but is not limited to, the following; the California Welfare and Institutions Code §10850, Information Practices Act - California Civil Code §1798 et seq., Public Records Act - California Government Code §6250 et seq., California Penal Code §502, 11140-11144, 13301-13303, Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) - 45 CFR Parts 160 and 164, and Safeguarding Information for the Financial Assistance Programs - 45 CFR Part 205.50. ENTITY agrees to comply with the laws applicable to the DOJ CURES data received.

Project Representative

Name (Printed): ____________________
Title: ____________________
Organization: ____________________
Email Address: ____________________
Phone: ____________________
Signature: ____________________
Date Signed: ____________________

Information Security Officer or designee

Name (Printed): ____________________
Title: ____________________
Organization: ____________________
Email Address: ____________________
Phone: ____________________
Signature: ____________________
Date Signed: ____________________